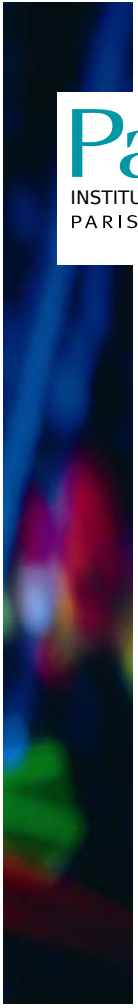
Communications Management in Cooperative Intelligent Transportation Systems

Manabu Tsukada



ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

MINES ParisTech

École doctorale n°432 : SMI–Sciences des métiers de l'ingénieur

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

l'École nationale supérieure des mines de Paris

Spécialité « Informatique temps réel, robotique, automatique »

présentée et soutenue publiquement par

Manabu TSUKADA

le 20 décembre 2011

Communications Management in Cooperative Intelligent Transportation Systems

Directeur de thèse : **Arnaud de LA FORTELLE**
Co-encadrement de la thèse : **Thierry ERNST**

Jury

M. Jean-Marie BONNIN, Professeur, Telecom Bretagne	Rapporteur
M. Kazutoshi FUJIKAWA, Professeur, NAIST	Rapporteur
M. Bertrand DUCOURTHIAL, Professeur, Université de Technologie de Compiègne	Examinateur
M. Arnaud de LA FORTELLE, Professeur, Mines ParisTech / INRIA	Examinateur
M. Thierry ERNST, Chercheur, Mines ParisTech / INRIA	Examinateur

MINES ParisTech
CAOR - Centre de Robotique
60 Boulevard Saint Michel 75006 Paris, France

T H È S E

Acknowledgments

It was not possible to complete this dissertation alone, I therefore take this space to thank all those who have supported me these last years. The doctoral dissertation has been done with many direct and indirect supports especially from Centre de Robotique (CAOR) in Mines ParisTech where the dissertation is submitted to, and IMARA team in INRIA Paris-Rocquencourt where I have spent the most of the time in the Ph.D research life. I would like to thank the two supervisors from both teams, Arnaud de La Fortelle (from CAOR) and Thierry Ernst (from IMARA). Arnaud always found the positive points of the work and this kept me alway optimistic for the progress during the entire Ph.D life. Thierry supported all aspects of the dissertation (research direction, idea, proofreading) and I would have never even started my Ph.D life in France without him in the first place.

This dissertation has taken many benefits from the various kind of collaborative works with all of the present and past IMARA members. I am grateful to Jong-Hyouk Lee, Satoru Noguchi, Olivier Mehani, Yacine Khaled, José Santa, JinHyeock Choi, Thouraya Toukabri, and Ines Ben Jemaa for sharing ideas, developing systems together, doing experiment together and co-authoring research papers. Let me also thank Armand Yvet, François Charlot and Carlos Holguin for their effort to keep the vehicles and equipment always operational and their support for experiments.

Participating EU project is one of the most interesting things I have found in the research life in France. I have learned many things from the process of building consensus among the partners who have different culture and way of thinking. Some of the discussion caused sharp conflicts between the partners, however I believe that the process allow us to reach higher result than one without it. I had chances to join three EU projects (ANEMONE, GeoNet and ITSSv6) during my Ph.D course and I thank again to my supervisors to let me in to these projects. First, I would like to thank to all the ANEMONE project members for developing the large scale IPv6 testbed. The evaluation of the dissertation also have largely benefited from their efforts. Many thanks especially to Nicolas Montavont, Antoine Boutet, Tanguy Ropitault, Jean-Marie Bonnin for co-authoring a research paper. Second, I would like to thank the GeoNet project members for designing, implementing and validating the IPv6 GeoNetworking implementations. Many thanks especially to Hamid Menouar, Wenhui

Zhang and Maria Goleva for co-authoring a research paper. Third, I would like to thank the ITSSv6 project members for the currently ongoing works.

Let me also thank the members in my previous laboratory in Keio University (Japan) for educating me about the domain of IPv6 based vehicular communication for about five years in bachelor and master course. Although there were no official relationship between Keio University for this dissertation, I believe the spirits from my earlier education deeply influenced the success of the dissertation. Many thanks to Jun Murai, Keisuke Uehara, Thierry Ernst for leading me to get Ph.D in France.

Last but certainly not least, I would like to profoundly thank my parents for their unconditional support and encouragement. I would not have completed this work without the love and support of my parents and to them I dedicate this work. I also wish to thank my brother Minoru, the success in his challenge always stimulates and energizes me. Thank you!

With the IMARA members in 2010

With the GeoNet project members in 2010

Abstract

Cooperative Intelligent Transportation Systems (ITS) are systems where the vehicles, the roadside infrastructure, central control centers and other entities exchange information in order to achieve better road safety, traffic efficiency and comfort of the road users. This exchange of information must rely on a common communication architecture. The ITS Station reference architecture has thus been specified in ISO and ETSI. It allows vehicles and roadside ITS stations to organize themselves into Vehicular Ad-hoc Network (VANET), presumably through IPv6 GeoNetworking using IEEE802.11p and to connect seamlessly to the Internet through any available access technology. Several paths may thus be available at a given vehicle ITS station to communicate with other ITS stations. Paths are of three types: direct path, optimize path and anchor path.

The objective of the study is to optimize the communication between ITS Stations by selecting the best available communication path. This requires first to gather information available locally at the ITS station (position, speed, application requirements, media characteristics, capabilities, path status, ...) and collected from neighbors ITS stations (position, speed, services, ...) and then to process this information through a decision-making algorithm.

First, we define a network module allowing the combination of IPv6 together with GeoNetworking. Second, we propose a cross-layer path selection management module. Our contributions are mapped to the ITS station reference architecture by defining the relation between the ITS station network and transport layer (which hosts our IPv6 GeoNetworking contribution) and the vertical ITS station cross-layer entity (which hosts the path selection decision-making algorithm). We specify the functions allowing the exchange of parameters through the Service Access Point (SAP) between the network layer and the management entity (MN-SAP). The parameters used at the cross layer ITS station management entity are abstracted in a way so that they are agnostic to the protocols used at the ITS station network and transport layer, therefrom allowing easy replacement of protocol elements (*e.g.* replacing NEMO by other mobility support protocol) or permutation of the network stack (IPv6 or GeoNetworking, a combination of both or other network stack).

Résumé

Les systèmes de transport intelligents (STI) coopératifs sont des systèmes où les véhicules, l'infrastructure routière, les centres de contrôle de trafic et d'autres entités échangent des informations afin d'assurer une meilleure sécurité routière, l'efficacité du trafic et le confort des usagers de la route. Cet échange d'information doit s'appuyer sur une référence d'architecture de communication commune. C'est dans ce but que l'architecture de station STI a été spécifié par l'ISO et l'ETSI. Le concept de cette architecture de référence permet aux stations STI-véhicules et stations STI-infrastructure de s'organiser dans un réseau véhiculaire ad-hoc (VANET), tout en utilisant des protocoles de communication tels que GeoNetworking IPv6 et IEEE802.11p ainsi que toute autre technologie d'accès afin de se connecter de manière transparente à Internet. Plusieurs chemins peuvent donc être accessible à une station STI véhicule pour communiquer avec d'autres stations STI. Les chemins sont de trois types: le chemin direct, le chemin optimisé et le chemin d'ancré.

L'objectif de cette étude est d'optimiser la communication entre stations STI en sélectionnant le meilleur chemin de communication disponible. Cela exige d'abord de recueillir les informations disponibles localement dans la station STI (la position, la vitesse, les exigences des applications, les caractéristiques des supports de communication, les capacités, l'état du chemin), ainsi que les informations des stations STI voisines (position, vitesse, services, etc.). Ces informations sont ensuite traitées par le biais d'un algorithme de prise de décision. Premièrement, nous définissons un module réseau qui permet la combinaison d'IPv6 avec le GeoNetworking. Deuxièmement, nous proposons un module de gestion inter-couches pour la sélection du meilleur chemin. Nos contributions s'intègrent dans l'architecture de station STI par la définition de la relation entre la couche réseau et transport (qui héberge la contribution GeoNetworking IPv6) et l'entité verticale de gestion inter-couches (qui accueille l'algorithme de décision pour la sélection de chemin). Nous avons spécifiés les fonctions permettant l'échange de paramètres par l'intermédiaire de le point d'accès au service (SAP) entre la couche réseau et l'entité de gestion (MN-SAP). Les paramètres utilisés dans l'entité de gestion inter-couches sont extraits d'une manière agnostique par rapport aux protocoles de la couche réseau et transport, ce qui permet de remplacer facilement les éléments d'une couche sans affecter les autres (par exemple, remplacer NEMO par une autre protocole de mobilité) et de permuter plusieurs piles réseau (on peut choisir d'utiliser la pile IPv6 ou bien la pile GeoNetworking, ou encore une combinaison des deux à la fois ou même une autre pile).

Contents

Résumé de la thèse en français

Contents

1 Introduction

1.1 Systèmes de transport intelligents coopératifs

Les systèmes de transport intelligents (STI) sont déployés pour optimiser le trafic routier et réaliser une mobilité humaine sécurisée, efficace et confortable. Différentes technologies sont appliquées aux STI, tels que les communications sans fil, la gestion des réseaux, les technologies de la sécurité des systèmes ou les technologies de détection. La recherche sur les STI a une longue histoire: Elle a commencé très tôt à partir de 1970, au Japon [FHWA1996]. Cependant, nous pensons que son déploiement va se réaliser dans un avenir proche grâce au déploiement du réseau mondial Internet, les technologies standardisés sans fils, l'amélioration du rendement et les équipement électronique à moindre prix. Les STI coopératifs sont un sous ensemble des STI: un système coopératif est un terme général pour les systèmes où plusieurs entités partagent des informations et des tâches pour réaliser des objectifs communs. Ainsi, les STI coopératifs sont un tel système basé sur l'échange de données entre les véhicules, l'infrastructure routière, les centres de contrôle de la circulation, les usagers, les administrations routières, les opérateurs routiers, etc. La Commission européenne (CE) a publié le plan d'action [EC-COM-886:Action-plan] en Europe suivie par son mandat de normalisation [EC-M/453].

Cette étude se concentre sur les STI coopératifs basés sur IP. Dans Internet, il y a peu de barrières entre les pays. Et les véhicules traversent les frontières, aussi particulièrement en Europe. Il est donc nécessaire que les STI coopératifs reposent sur les mêmes architecture, protocoles et technologies. En tant que tel, beaucoup d'organismes de standardisation se sont concentrés sur le développement des normes pour les STI coopératifs. L'IETF (Internet Engineering Task Force) est une organisation mondiale de travail pour la normalisation des protocoles de l'Internet. En outre, l'organisation internationale de normalisation (ISO) et particulier le Comité technique 204 groupe de travail 16 (TC204 WG16) (aussi connu sous le nom de CALM) est en charge de la normalisation d'une architecture de communication pour STI coopératifs. Le TC204 WG16 travaille spécialement sur une architecture de communication qui offre plusieurs technologies d'accès et plusieurs applications. En Europe, l'European Telecommunications Standards Institute (ETSI) TC ITS travaille sur le renforcement des blocs de la même architecture de manière à atteindre une harmonisation avec la norme ISO TC204 WG16. En 2010, l'ISO TC204 WG16 et ETSI TC ITS ont défini l'architecture de référence station STI [ISO-21217-CALM-Arch, ETSI-EN-302-665-Arch].

1.2 Motivations et Objectifs

L'objectif de l'étude est d'optimiser la communication entre les entités communicantes en sélectionnant le chemin le plus approprié à l'aide des informations échangées par les STI coopératifs basées sur IP. Nous considérons que la sélection du chemins d'accès approprié est la décision la plus importante pour optimiser la communication entre stations STI. Afin de rendre la contribution de cette étude plus extensible, les paramètres du processus de prise de décision sont extraits de n'importe quel protocole réseau ou technologie radio (par exemple une adresse IP est considérée comme un identifiant ou un localisateur selon le rôle qu'il joue). Nous avons également défini l'interaction entre le processus de prise de décision et les types d'informations. Le transfert de paramètres via les points d'accès au service (SAPs) est définit par rapport à l'architecture de référence station STI standardisé par l'ISO et l'ETSI.

2 Contexte et état de l'art

Nous avons pris connaissance des organisations de normalisation et les programmes de recherche en Europe et dans le monde. Parmi les organismes de normalisation, nous avons trouvés que l'ISO, l'ETSI et l'IETF fournissent les normes les plus pertinentes pour cette étude. Le programme cadre est le plan de recherche menée par la Commission européenne, au sein du quel les projets CVIS, GeoNet, ANEMONE, ITSSv6 et DriveC2X sont des facteurs clés du domaine des STI coopératifs. Le Consortium Car-to-Car Communication Consortium (C2C-CC) est un forum de industriel initié par l'industrie automobile européenne. COMeSafety est un effort d'harmonisation en vue de consolider les résultats des projets précédents. Cette consolidation a conduit à la spécification de l'architecture de station STI de référence et sa normalisation par la norme l'ISO et l'ETSI. Cette étude suit cette architecture ainsi que la terminologie utilisée par l'ISO et l'ETSI. L'architecture se repose sur quatre sous-systèmes (les stations STI-véhicule, bord de route, centrale et personnelle). La coopération de ces stations STI permet d'atteindre l'objectif commun des STI coopératifs. Pour discuter de la communication entre les stations STI , trois modes de communication sont définis: communication basée sur les véhicules, communication basée sur les stations de bord de route et communication via Internet.

Pour aperçu de toutes les technologies possibles nécessaires aux ITS coopératifs, les technologies de réseau et les technologies d'accès, ainsi que les couches physique et liaison pour les technologies sans fil sont résumées puis différents protocoles réseau sont expliqués. Comme protocoles de couche réseau, une taxonomie est proposé où les protocoles sont principalement divisés en classes avec st sans infrastructures. La classe sans l'infrastructure est connue par le secteur de la recherche sous le nome de Mobile Ad-hoc Network (MANET). Comme les protocoles de routage MANET, ceux de topologique et géographique sont expliqués. Les mécanismes d'auto-configuration d'adresse et de découverte de réseau dans le véhicule sont présentés comme un contexte de MANET. Les protocoles reposant sur des infrastructures sont classés en trois catégories: Support à la mobilité à Internet, l'amélioration de la mobilité et autres. Support à la mobilité Internet est un ensemble de technologies pour permettre aux applications des nœuds mobiles d'utiliser une adresse IP stable comme un *identifiant* tandis que les paquets IP sont acheminés selon d'autres adresses de *Localisateur* dans la topologie logique. Nous expliquons la technologie clé de la thèse, NEMO et la technologie de mobilité tout autre support. L'amélioration de la mobilité est un ensemble de technologies utilisées, avec le support de mobilité Internet pour fournir une meilleure communication aux nœuds mobiles.

3 Énoncé du problème et des exigences de conception

Tout d'abord, trois questions sont présentées. La sélection de chemins est une question de prise de décision: le choix d'un chemin d'accès approprié adapté aux exigences des applications à partir des chemins multiples existent entre le véhicule stations STI. Le processus de sélection de chemins doit être effectué comme la combinaison des sélections de différents paramètres (Interface de communication, localisateur, routeurs d'accès, de routage et d'ancrage). Pour permettre la sélection de chemins intelligents, l'information géographique joue un rôle important. La gestion de position géographique est une question sur la façon de propager et de gérer l'information géographique dans stations STI. Pour combiner IPv6 et GeoNetworking, nous sommes confrontés à de nouvelles questions d'adressage et de routage. Pour réaliser le GeoNetworking sur IPv6, nous devons aussi étudier comment les paquets IPv6 sont livrées par GeoNetworking sans IPv6 sensibilisation afin de ne avoir pas trop d'impact sur l'architecture de station STI.

Ensuite, nous expliquons ce que sont les exigences de conception pour la solution. La solution doit suivre l'architecture de station STI gardant l'indépendance des couches. Les paramètres et les messages échangés entre les couches doivent être souples et abstraits autant que possible pour faciliter les extensions futures. Nous suivons le concept de station STI hôte routeur et partagé où le routeur station STI est en charge de la communication pour toute la station STI. Les hôtes qui exécutent des applications sont ainsi libérés de la gestion de la communication. La solution de GeoNetworking IPv6 doit prendre en charge tous les nouveaux types de communications de routage géographique. Pour supporter le GeoNetworking IPv6, la gestion doit abstraire le GeoNetworking pour l'hôte de station STI d'exécuter les applications. Station STI doit être en mesure de changer de point d'attache un lien vers un autre sans interrompre sessions IP en cours. Le support à savoir la mobilité du réseau est nécessaire. Les chemins doit être utilisés conformément aux exigences des applications et des chemins multiples peuvent être utilisés simultanément.

4 Conception des solutions

Afin d'optimiser la communication entre stations STI coopératifs basées sur IP, nous avons besoin pour répondre aux six questions suivantes: Quelle est l'information fondamentale exigée par l'Entité du Gestion de Station STI (EGS), d'où l'information vient, quelles informations sont maintenues dans la couche réseau, comment les informations de réseau sont fournie à l'EGS, comment le chemin est sélectionné et comment IPv6 et GeoNetworking sont combinés. Pour répondre à ces questions, nous examinons comment les paramètres de la couche réseau sont résumés dans l'entité de gestion et la façon dont les paramètres sont transmis entre l'EGS et la couche réseau. Cette étude nous conduit à définir trois tableaux dans l'EGS: la table d'informations Station STI, la table d'informations chemins et la table d'exigence de flux. Nous identifions également que quatre primitives qui sont nécessaires pour l'interaction entre l'EGS et la couche réseau. Deux d'entre elles sont nécessaires pour instruire la couche réseau de passer un flux sur un chemin donné et correspondent à des primitives déjà définis dans les normes l'ISO (MN-REQUEST et MN-COMMAND) pour un bloc de protocole de couche réseau autre que IPv6, tandis que deux nouvelles sont nécessaires pour accéder à l'information contenue dans les bases d'information de gestion (MIB) déjà définies dans les blocs de protocole de couche réseau IPv6. Un agent d'adaptation est nécessaire dans le bloc de protocole IPv6 dans le but d'échanger les informations avec l'EGS et de traiter des instructions en provenance de l'EGS.

Nous étudions ensuite la manière dont le meilleur chemin est sélectionné. La sélection de chemins est réalisée dans l'Entité du Gestion Station STI selon les exigences des applications enregistrées dans la table d'exigences de flux, l'état du réseau et les informations d'interface enregistrées dans la table des informations de chemin. Il est important pour la sélection intelligente de chemin de prévoir la trajectoire du véhicule et ses caractéristiques. La prédiction effectuée par l'EGS est stockée dans la table des informations de chemin. Enfin, nous examinons comment IPv6 et GeoNetworking sont combinés. Les paquets IPv6 sont encapsulés dans des paquets GeoNetworking par le routeur GeoNetworking de Station STI qui est responsable de les communications de l'ensemble de la station STI de manière transparente GeoNetworking pour les hôtes de la station STI. Une interface interne de la couche réseau est nécessaire pour transmettre des paquets entre IPv6 et GeoNetworking (GeoIP SAP). À la suite de cette étude, un modèle d'abstraction pour l'interaction entre la gestion et réseau est présenté. Enfin, nous concluons ce chapitre en montrant comment les trois contributions majeures (soit le gestionnaire de sélection de chemins, paramètres inter-couches de sélection de chemins et primitives et mécanismes du GeoNetworking IPv6) vont être présentées dans les chapitres suivants .

5 Gestionnaire de sélection de chemins

Notre intérêt principal est d'offrir la décision intelligente de sélection de chemins à toutes les applications qui s'exécutent sur les hôtes Station STI, tout en gardant le processus de décision indépendant de tout protocole de couche réseau spécifique. Le processus de décision est principalement divisé en deux parties: les entrées de paramètres abstraits de la couche réseau à partir des points d'accès au service (SAPs) dans les paramètres de gestion, et la sortie vers les blocs de la couche réseau du protocole basée sur la décision. Tout d'abord, nous présentons trois paramètres de gestion nécessaires à la prise de décision: la table d'informations Station STI, la table d'informations des chemins et la liste d'exigences des applications. La table d'informations de stations STI et la table d'informations des chemins sont nouvellement

définis à la suite des approches de la suite de travaux chapitre 5, tandis que la liste d'exigences des applications est étendue à partir de ce qui a été définie dans la norme ISO.

Puis, nous introduisons la façon dont le chemin est sélectionné basé sur ces paramètres de gestion. La sélection de chemins est encore divisé en phase de calcul du chemin et de prise de décision. Dans la phase de calcul du chemin, tous les chemins candidats sont calculés en fonction des informations sur les interfaces de communication, localisateurs topologiques, relais suivants (next hop), ancres, et des capacités. Toujours dans cette phase, la disponibilité des chemins est estimée d'après des informations diverses. À titre d'exemple, nous présentons une estimation basée sur l'information géographique de disponibilité du chemin. Les résultats du calcul du chemin candidat et l'estimation de disponibilité sont stockées dans la table des informations de chemin. Dans la phase de prise de décision, une méthode de décision Multiple Attribute Decision Making (MADM) employée dans l'algorithme de sélection de chemins. Les décisions sont transmises à la couche réseau.

6 Paramètres inter-couches de sélection de chemins

Quatre primitives sont nécessaires pour l'interaction entre l'entité de gestion de Station STI (EGS) et la couche de Réseau et transport de station STI (RTS). Premièrement, nous proposons deux nouvelles primitives (MN-GET et MN-SET) permettant au gestionnaire de sélection de chemins à certains des paramètres (N-Paramètres) enregistrées dans la base de gestion d'information existante (MIB) de IPv6 et de protocoles TCP et UDP. Les deux autres (MN-REQUEST et MN-COMMAND) sont nécessaires pour charger le bloc protocole IPv6 de passage des flux à un chemin donné et correspondent aux primitives déjà définies dans les spécifications ISO pour un bloc de protocole de couche réseau autre que IPv6 (ex. FAST). Nous avons donc étendu ces primitives pour transférer les informations nécessaires entre le gestionnaire de sélection de chemins et les blocs IPv6, GeoNetworking et protocoles TCP/UDP de la RTS. Nous notons que la spécification ISO actuelle des commandes MN-REQUEST et MN-COMMAND ne répond pas à nos exigences de conception décrites dans le chapitre 4. Aussi, nous définissons cinq nouvelles commandes MN-REQUEST (*STAGeoNot*, *STATopoNot*, *STAServNot*, *PathNot*, et *PathMetricNot*) et trois nouvelles commandes MN-COMMAND (*STAServDiscov*, *PathMNG*, *FlowPolicy*) pour satisfaire nos besoins pour la sélection de chemins.

Puis nous expliquons comment ces commandes sont effectivement utilisés. Pour ce faire, nous présentons d'abord la correspondance entre les paramètres abstraites contenus dans les tables d'exigence de flux, d'information de Station STI, et d'informations de chemin dans l'entité de gestion de Station STI et les paramètres correspondants dans le blocs de protocole IPv6 et de GeoNetworking. Puis, pour montrer l'interaction entre l'entité de gestion et de la couche réseau, nous décrivons la procédure complète de sélection de chemins, d'activation d'interfaces de communication et la transmission des instructions de politique de flux.

Le lecteur notera que cette étude est basée sur les versions des normes ISO de l'année 2011 et que les normes évoluent constamment. En conséquence, les primitives et les paramètres de la MN-SAP peuvent avoir changé au moment de la lecture.

7 Interaction d'IPv6 et de GeoNetworking

Nous passons d'abord en revue les modules fonctionnels et les interfaces entre les entités qui composent l'architecture GeoNetworking IPv6 telle qu'elle sont définies dans le projet

GeoNet. Suite à l'approche présentée dans le chapitre 5, le module GeoNetworking est défini comme une couche directement inférieure de l'IPv6. GeoNetworking apparaît donc comme une couche d'accès et est présenté à l'IPv6 sous la forme d'une interface de communication avec des capacités de GeoNetworking. Les paquets IPv6 livrés dans un VANET où GeoNetworking est utilisé comme protocole de routage multi-sauts sont donc encapsulés dans un paquet GeoNetworking par le routeur de station STI qui est responsable de la communication de l'ensemble de la station STI et gère GeoNetworking de manière transparente par les hôtes de la station STI. Une interface interne à la couche réseau est nécessaire pour transmettre les paquets entre IPv6 et GeoNetworking. Nous avons donc spécifié le point d'accès au service GeoIP (GeoIP-SAP) entre GeoNetworking et IPv6. Dans le SAP GeoIP, les paquets IPv6 sont mappés à l'un des quatre types de communication (GeoUnicast, GeoBroadcast, GeoAnycast, TopoBroadcast) en fonction de l'adresse IP de destination. Enfin, afin d'alléger les contraintes qu'un sous-réseau IPv6 est limité à une zone géographique, nous proposons la fin du modèle basé sur le lien géographique. Dans le modèle de lien proposé, l'adresse IP utilisée pour le mode de communication routière est déterminé par chaque véhicule de station STI avec des informations plus précises du véhicule.

8 Exécution

Tous les modules sont mis en œuvre dans un routeur de station STI basé sur le système d'exploitation Linux. Nous introduisons le base de données sur les politiques de routage (RPDB) pour IPv6, afin de permettre l'utilisation simultanée de plusieurs chemins d'accès (par exemple autre véhicules, en bordure de route et basée sur Internet), qui est l'une des exigences de conception décrites dans le chapitre 4. Trois différentes implémentations du GeoNetworking ont été développées au cours de cette thèse: deux d'entre elles ont été mis en œuvre dans le cadre du projet GeoNet, et l'autre a été mises en œuvre par collaboration entre l'équipe IMARA (France) et Espritec (Tunisie). Nous avons fourni un exemple de code de GeoIP-SAP défini dans le chapitre 8 pour toutes les implémentations et dirigé la validation de toutes les implémentations. Les paquets IPv6 sont transmis au module de GeoNetworking par l'intermédiaire d'une interface virtuelle TUN. Cette interface virtuelle permet de traiter le module GeoNetworking comme l'une des interfaces de communication du point de vue d'IPv6. Le gestionnaire de sélection de chemins décrit dans le chapitre 6 a été partiellement mis en œuvre comme une extension de implémentation open-source NEMO (NEPL). L'estimation de disponibilité du chemin décrite dans le chapitre 6 est utilisée pour sélectionner le routeur d'accès approprié.

La mise en œuvre de l'utilisation simultanée de plusieurs chemins est publiée dans [Tsukada2008, Tsukada2010a], et les détails des deux implémentations GeoNetworking IPv6 dans le cadre du projet GeoNet peuvent être trouvé dans [GeoNet-D.3, Tsukada2010b, Ines2010]. L'autre exécution de GeoNetworking IPv6 est publié en open source CarGeo6 [Toukabri2011].

9 Évaluation

La première section décrit les quatre grands objectifs et la deuxième section présente la méthodologie utilisant des environnements de test à l'intérieur et extérieur jusqu'à quatre véhicules. Les détails des tests effectués sont présentés dans la section suivante. Les objectifs sont de mesurer, l'amélioration du rendement l'utilisation simultanée de plusieurs chemins, la surcharge induite par l'usage de GeoNetworking IPv6, la surcharge en utilisant NEMO

sur GeoNetworking IPv6 et d'analyser les différents grâce à affecte des conditions sur les métriques. Ensuite, la configuration du réseau, la plate-forme des véhicules, des paramètres, (round-trip time, débit, gigue, taux de livraison de paquets, nombre de sauts) et les scénarios d'expérimentation sont décrits. Nous avons développé un outil d'analyse des paquets et de visualisation appelé AnaVANET afin de comprendre l'effet de l'état de différents paramètres pour les évaluation d'essai à l'extérieur.

Le chapitre 11 présente les évaluations de MANEMO, à savoir la combinaison de MANET et NEMO et montre que cela offre un certain nombre d'avantages, tels que l'optimisation des itinéraires ou la multi-connexion. Dans le but d'évaluer les avantages de cette synergie, ce chapitre présente une solution basée sur des politique de répartir de trafic entre plusieurs chemins pour améliorer la performance globale d'un réseau de véhicules. Un banc d'essai des véhicules a été développé pour effectuer des essais sur le terrain. Tout d'abord, la performance de l'Optimized Link State Routing (OLSR) est évaluée dans un VANET avec un maximum de quatre véhicules comme point de repère afin de comparer avec GeoNetworking IPv6 dans les mêmes conditions dans le chapitre suivant. AnaVANET est utilisé pour analyser l'impact de la position des véhicules et de la circulation sur les performances du réseau. Les résultats de performance ont été géo-localisé en utilisant les informations GPS. Deuxièmement, en passant de chemin ancré (chemin NEMO) et à le chemin direct (chemin d'accès OLSR), les chemins entre les véhicules sont optimisés et la performance finale est améliorée en termes de latence et de bande passante. Nos résultats expérimentaux montrent que l'exploitation du réseau est encore améliorée avec l'utilisation simultanée de NEMO et MANET.

Le chapitre 12 présente une évaluation expérimentale de le GeoNetworking IPv6 sur une pile mise en œuvre par Hitachi et NEC par le projet GeoNet. Nous avons effectué nos expériences à la fois sur un banc d'essai à l'intérieur et le banc d'essai en plein air pour évaluer les performances du réseau IPv6 sur GeoNetworking . L'environnement de test à l'intérieur est conçu pour évaluer les performances pure d'IPv6 sur GeoNetworking en évitant les interférences dues à des perturbations radio inattendues. Nous avons mesuré les performances du réseau avec UDP, TCP et ICMPv6 trafic à l'aide *iperf* et *ping6*. Considérant le test en plein air, nous pouvons voir que le protocole IPv6 sur GeoNetworking functionne comme la spécification dans les scénarios de conduite. La communication est stable, même lorsque la vitesse du véhicule est d'environ 100 kilomètres par heure et quand la vitesse relative entre les véhicules est élevée. La portée radio est plus grande que prévu. La portée maximale de communication est d'environ 450 mètres et elle n'est pas interrompu par les bâtiments sur le campus INRIA (un seul étage).

Dans le chapitre 13, nous décrivons les résultats de l'évaluation de la mesure du rendement de la mise en œuvre CarGeo6, par le biais de l'évaluation expérimentale de banc d'essai à l'intérieur et le banc d'essai en plein air. La configuration basique de l'évaluation est commun avec le test effectué dans le chapitre précédent en utilisant les implémentations GeoNet. Ainsi l'on compare les différences de performance. Avec le banc d'essai en plein air, nous évaluons la performance de la communication par Internet en combinant CarGeo6 et NEMO. Les mesures de la performance sont traitées et analysées avec AnaVANET. Plus de détails sur les tests à l'intérieur sont publiés dans [Toukabri2011].

10 Conclusions

Dans cette thèse, nous avons étudié comment la communication entre un véhicule et ses pairs peut être optimisée en sélectionnant le chemin de communication approprié à l'aide tous les types possibles d'information en matière de STI coopératifs. Tout d'abord, nous avons

présenté toutes les pièces sur lesquelles ce travail est basé: les activités des STI coopératifs, la terminologie, l'architecture de référence de Station STI, les technologies de couche d'accès et les protocoles de couche réseau, en particulier IPv6 et les protocoles de mobilité (partie I). Dans le chapitre 4, nous avons mis en évidence les problèmes et les exigences de conception pour réaliser la sélection intelligente de chemins et GeoNetworking IPv6 sein de l'architecture station STI. Nous avons conclu que la sélection de chemins a besoin de gérer trois types de chemins entre les véhicules: chemin ancré, chemin optimisé et chemin direct. Nous avons proposé une sélection inter-couche du chemin et une amélioration de l'algorithme de la prise de décision utilisant des informations provenant des diverses couches de la pile station STI. L'étude a mené à trois grandes propositions: une gestionnaire de sélection de chemins (chapitre 6), les paramètres inter-couches de sélection de chemins (chapitre 7) et une interaction d'IPv6 et de GeoNetworking (chapitre 8).

Afin d'adapter ces propositions dans l'architecture ISO/ETSI de station STI, nous avons proposé l'approche d'abstraire les paramètres échangés entre l'entité de gestion et de la couche réseau (chapitre 5). Selon cette approche, il est possible de concevoir une définition des paramètres échangés plus complète que de se contenter d'énumérer les paramètres pour répondre aux besoins comme peut être trouvé dans les spécifications ISO en vigueur. Dans ce dissertation, nous nous sommes concentrés sur les paramètres liés à la sélection de chemins, mais l'approche peut être appliquée à des sujets autres (ex. qualité de service, multidiffusion, etc.). L'approche présentée peut être une référence pour la conception de l'échange de paramètres entre les autres couches et de l'entité de gestion (ex. MF-SAP et MI-SAP). C'est parce que notre approche d'abstraction rend les fonctions inter-couches indépendant de tout protocole spécifique.

Nous considérons que les principales contributions de cette thèse sont:

- La proposition d'un système permettant de combiner l'IPv6 et GeoNetworking afin de profiter à la fois des avantages de chaque protocole. Les paquets IP unicast, multicast, et anycast sont encapsulés dans les pacqués GeoNetworking correspondants selon un mapping particulier. La proposition d'un algorithme de gestion inter-couche pour la sélection du chemin qui interagit avec des composants qui permettent d'assurer le routage réseau logique, un routage et l'adressage géographique et de fournir les caractéristiques de la liaison sans fil et la performance.

- La définition de l'interface (point d'accès au service) entre la fonction de décision inter-couche et la couche réseau en conformité avec les spécifications ISO / ETSI.

- L'implémentation de l'interface entre IPv6 et GeoNetworking définie dans le projet GeoNet et son intégration dans trois piles GeoNetworking différentes. Elle a aussi été validé sur un banc d'essai composé de plusieurs véhicules testés dans un environnement réel. Une évaluation de la performance de GeoNetworking IPv6 a aussi été effectuée.

- La conception et la mise en œuvre du point d'accès au service pour GeoNetworking IPv6. La spécification de le SAP définie dans le projet GeoNet a été mise en œuvre sur une station STI-véhicule basée sur Linux. La mise en œuvre est testée et vérifiée sur des véhicules dans un environnement réel. La performance du réseau est aussi mesurée pendant les expérimentations.

- Le développement d'un outil d'évaluation et de visualisation nommé AnaVANET qui permet d'évaluer les réseaux véhiculaires. AnaVANET retrace tout les paquets de données transmis ou retransmis par les véhicules. Il détecte ainsi les pertes de paquets,

génère à la fois des statistiques de bout en bout et par-hop, et permet de relier les métriques de la couche liaison jusqu'à la couche transport ainsi que les métriques géographiques tels que la vitesse, la position et la distance.

Enfin, nous fournissons le perspective pour faire avancer les travaux qui ont été fait sur la thèse. Nous ouvrons également les autre questions importantes liées au thème que nous avons découvert au cours de la thèse.

Chapter 1

Introduction

Contents

1.1 ICT and automotive

In 2008, 1.2 million of people were killed by road traffic accidents worldwide, which is the ninth cause of human deaths and is corresponding to 2.2% of the total number of human death [WHO2008]. 50 millions were injured in road traffic accidents, which is the eleventh cause of injury worldwide [WHO2004]. In Europe, traffic accidents kill 43000 citizens and 1.8 millions are wounded every year. The social cost of the accidents is more than 160 billion euros which is equivalent to 2% of Gross Domestic Product (GDP) in Europe [EC-CARE-database2008].

Beside fatal accidents and injuries, the other social costs include energy consumption and gas emission. In 2002, the transport sector consumed 338 million tonnes oil equivalent (MToe) representing 31% of the total energy consumption in the European Union. Road transport consumed 281 MToe, or 83% of the energy consumed by the whole transport sector. Road transport CO_2 emissions account for 835 million tonnes per year representing 85% of the total transport emissions [Intelligent-Car-Initiative2006].

Current transportation systems have a very unfavorable impact on the society including not only traffic accidents but also air pollution, energy consumption, noise disturbance, etc. Providing an answer to these issues is key for improving the quality of life. In February 2006, the Intelligent Car Initiative was presented by the European Commission to improve the transportation system using Information Communication Technologies (ICT).

The integration of ICT technologies and automotive technologies has a huge impact not only on research but also on the industry sector. Currently, 950 million vehicles are registered worldwide, 230 million of them are in the enlarged European Union, 250 millions are in the United States and 75 millions are in Japan [ACEA2008, JAMA2009]. A vehicle may embed hundred of sensors and mobile devices brought by passengers. These computers are going to communicate and cooperate using ICT technologies. The impact of ITS is not only on the transportation system side, but also on the data communication network side. When a huge

number of computers are connecting to the network, the data communication network side must be designed to accommodate the communication traffic.

Figure 1.1 and Figure 1.2 show the share of the investments between sectors for research and development in EU and Japan [i2010, JRC-IPTS2009, JAMA2009]. The shares of the investment into the automotive and ICT sectors are the first and the second among all sectors in both EU and Japan. The total percentage of automotive and ICT sectors reaches up to more than 40% in both EU and Japan. This can be seen a an evidence that the integration of automotive and ICT technology is anticipated.

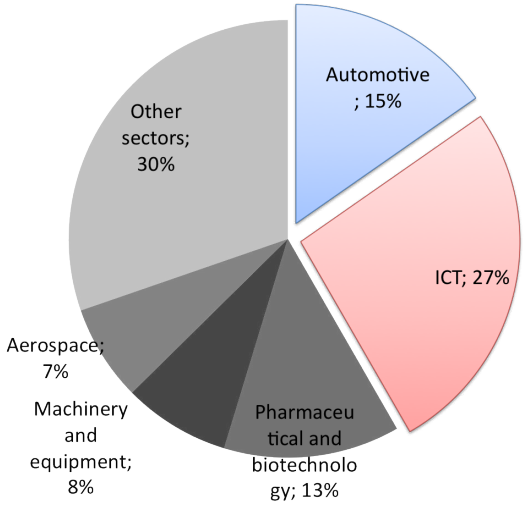


Figure 1.1: Investment of R&D in EU

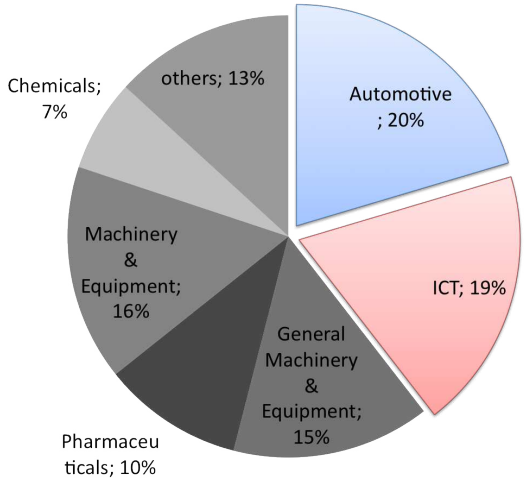


Figure 1.2: Investment of R&D in Japan

Intelligent Transportation Systems (ITS) are systems deployed to optimize the road traffic and realize safe, efficient and comfortable human mobility. Various technologies are applied to ITS including wireless communications, network management, security technology, Computational technologies, sensing technologies, etc. Research on ITS has a long history. The early stage research started from 1970s in Japan [FHWA1996]. However, we believe that ITS deployment will come true in the near future thanks to the largely deployed Internet, standardized wireless technologies, performance improvement of computer with cheaper price, etc.

Cooperative ITS is a particular case of ITS: a Cooperative system is a general term for a system where multiple entities share information and tasks to achieve common objectives. Thus Cooperative ITS is the system to achieve ITS objectives based on the data exchange between vehicles, the roadside infrastructure, traffic control centers, road users, road authorities, road operators, etc. The European Commission (EC) published the action plan [EC-COM-886:Action-plan] in Europe followed by ITS standardization mandate [EC-M/453].

1.2 IP-based Cooperative ITS

To share the data between the various ITS components (vehicle, roadside, center, etc.), there are mainly two approaches either using IP and without using IP. The non-IP approach puts more importance to the network performance such as delay, packet delivery ratio and so on by omitting the IP header and processing at the IP layer. On the other hand, IP provides

more interoperability, open innovation, flexibility, ease of deployment and so on. In 2011, the Cooperative ITS community considers both approaches are necessary to realize the various scenarios for Cooperative ITS. When it comes to IP, IP version 6 [rfc2460] is considered as necessary to fulfill cooperative ITS requirements thanks to its extended address space, embedded security, enhanced mobility support and ease of configuration.

This study focuses on IP-based Cooperative ITS. First, the existing applications are working on IP, and the development tools and developers' skill for applications using IP are accumulated over the past years. This fact gives more chance to open the door of innovation when IP based Cooperative ITS gets deployed. In addition to ease the deployment and development, IP is a convergence layer that hides the difference of underlying layers. IP can provide a transparent interface to upper layers even when new access technologies are deployed. In the future, Cooperative ITS may interact with other systems such as education systems, health care systems, broadcast systems, etc. Cooperative ITS based on IP provides a room for interoperability with the other IP-based systems, and will effectively lead cooperative ITS to become part of the Internet of things.

In the Internet, there are few barriers among countries, and vehicles easily cross the country borders, especially in Europe. Thus there is a huge necessity that Cooperative ITS rely on the same architecture, protocols and technologies. As such, standardization organizations are developing cooperative ITS standards. The Internet Engineering Task Force (IETF) is the worldwide organization working for standardization of protocols in the Internet. The International Organization for Standardization (ISO) Technical Committee 204 Working Group 16 (TC204 WG16) (also known as Communications Architecture for Land Mobile (CALM)) is in charge of standardizing a communication architecture for cooperative ITS. TC204 WG16 is specially working on an a communication architecture supporting all type of access media and applications. In Europe, the European Telecommunications Standards Institute (ETSI) TC ITS is working on building blocks of the same architecture in harmonization with ISO TC204 WG16. In 2010, both ISO TC204 WG16 and ETSI TC ITS defined the ITS Station reference architecture [ISO-21217-CALM-Arch, ETSI-EN-302-665-Arch]. The architecture is detailed in section 2.2.

The ITS Station reference architecture looks like the layered Open Systems Interconnection (OSI) reference architecture. In the networking and transport layer which is the focus of this study, IPv6 is considered as a necessary protocol block to accommodate all cooperative ITS requirements *e.g.* Internet connectivity must be maintained while vehicles changes their point of attachment to the network as they move. The continuous change of point of attachment causes the applications running in the vehicle to break their sessions unless mobility support mechanisms are provided. IETF has standard Internet mobility protocols to solve the problem. Because vehicles may embed several nodes connected to an in-vehicle network, mobility support must be provided to all the nodes. Network Mobility (NEMO)[rfc3963] has thus been specified by the IETF NEMO Working Group as a network mobility protocol and adopted by ISO TC204 WG16 to achieve Internet mobility for vehicles [ISO-21210:2011-CALM-IPv6].

The network and transport layer of the ITS Station reference architecture also comprises non-IP network protocols specialized in specific ITS communication in the scenarios. GeoNetworking is proposed in order to improve the routing performance in dynamic network topologies such as Vehicular Ad-hoc Network (VANET). In GeoNetworking, the geographic position of the vehicle is used in order to route the packets for Vehicle-to-Vehicle (V2V) and Vehicle-to-Roadside (V2R) communications. Despite its strength for dynamic network topology, GeoNetworking does not have the advantages of IP described above (ex. GeoNetworking

is not interoperable with other IP-based systems). Therefore, there is strong need to take advantage of both IP and GeoNetworking and combine them.

On the other hand, vehicle ITS Station may be equipped with multiple wireless network interfaces in order to connect to other ITS Stations from anywhere and at anytime. As of today, no single wireless technology can fulfill all requirements in all ITS scenarios, however vehicle ITS Station can supplement limitation, instability and low performance of wireless technology with multihoming technologies by combining different types of wireless interfaces. When a vehicle ITS Station has several paths to communicate with other ITS Stations including Internet technologies, GeoNetworking technologies and access network technologies, the most appropriate path shall be selected. There is strong demand to make an intelligent decision to combine these technologies.

1.3 Objectives and Contributions

The objective of the study is to optimize the communication between vehicle and its communication peers by selecting the appropriate communication path using all possible types of information exchanged by IP-based cooperative ITS. Figure 1.3 shows information involved in the process of the path selection decision.

The decision should be based on vehicle and device hardware information, because, for example, opposite decisions may be taken, when the engine of vehicle is running, or when the engine is stopped. Affiliation and social role also should differentiate the decision-making process because non-private vehicles (ex. bus, police, ambulance) do not need strong anonymity for location privacy contrary to personal vehicles. When the communication peer is directly detected by computer vision using video camera or radar equipped in the vehicle, it may decide to discover the direct path to the communication peer rather than keeping the path via the Internet, because the communication peer is located physically near (in camera/radar range). Thus the path selection decision should also be taken based on the information provided by computer vision. The economy and monetary factor is also important for users. Some contracts of telecommunication operators provide different pricing for daytime and nighttime, and for the location of user (own country or foreign country). Thus the routing should be taken depending on the time, the location and user's policy. To increase user satisfaction, human factor and psychology also should be taken into consideration. The change from a low-bandwidth wireless interface to a high-bandwidth one may not give satisfaction to the user even when it transfers more data at a given time that is usually better for background traffic. The user may feel more comfortable with constant data transfer without changing the interface. As described earlier, these factors observed in the types of information are important for path selection decision-making process.

In this study, we mainly focus on the following four types of information while taking the other types of information to be taken into account in the future (In Figure 1.3).

- Application requirement and User demand,
- Logical Network Routing,
- Geographic addressing and routing,
- Wireless link characteristics and performance

We consider that selecting the appropriate path is the most important decision to optimize the communication between ITS Stations. In order to make the contribution of this study

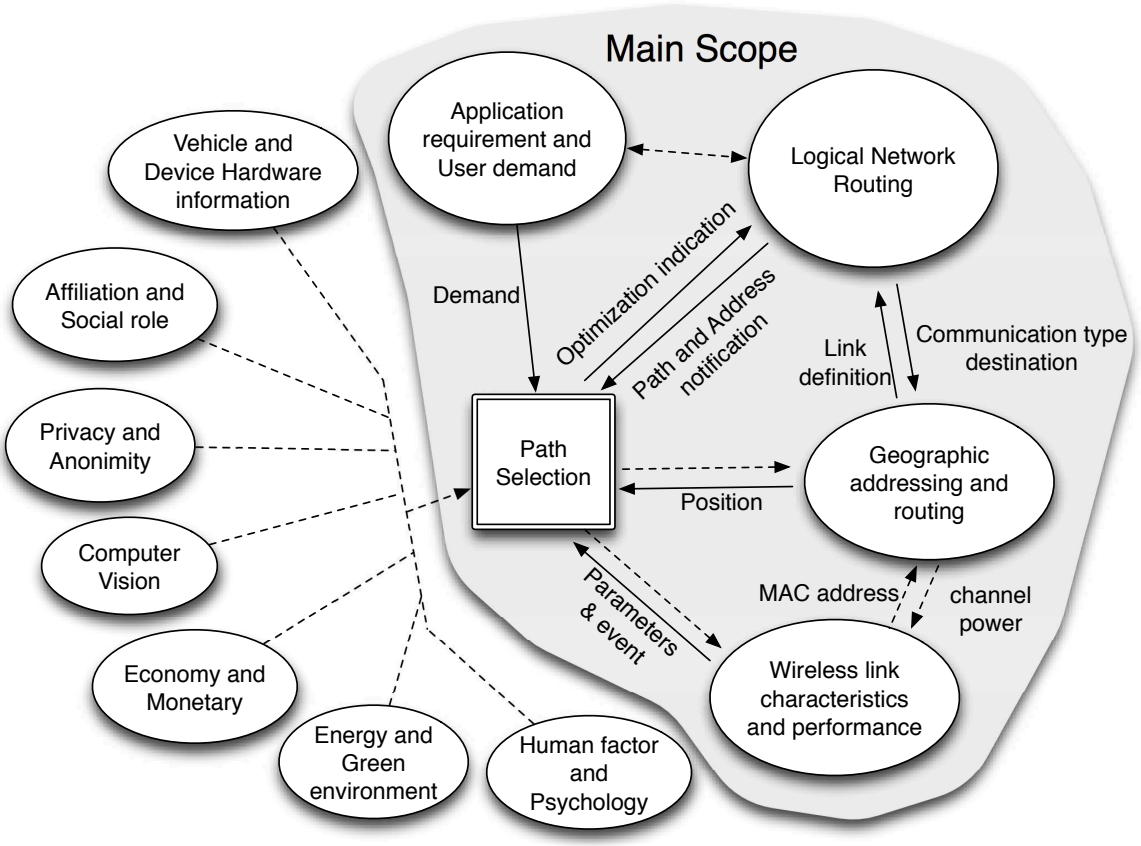


Figure 1.3: Decision-making process related types of information and the focus of this study

more extensible, the decision-making process parameters are abstracted from any particular network protocol or radio technologies (e.g. an IP address is considered an identifier or a locator according to the role it plays). We are also defining the interaction between the decision-making process and the types of information. The transfer of parameters via the Service Access Points is defined to fit to the ISO/ETSI ITS Station reference architecture.

As a first contribution, the State of the Arts analysis provides an overview of all the possible technologies needed in cooperative ITS including network technologies and access technologies. The analysis allows us to define the problem statement. First three main issues are identified, and then the solution design requirements are presented.

As a solution to the first issue, we propose a scheme to combine IPv6 GeoNetworking in order to take advantage of both IP and GeoNetworking. The scheme allows IP packets to be encapsulated and transferred in a multi-hop fashion without requiring treatment at the IP layer of the intermediate nodes. Unicast, multicast, anycast IP packets are encapsulated and mapped into GeoNetworking specific communication types. The interaction between IP and GeoNetworking is considered as the one between *logical network routing*, and *geographic addressing and routing* in Figure 1.3. Note that we contributed to the development of the interaction between IPv6 and GeoNetworking under the framework of European Project ((See details in Section2.1.2.1) coordinated by INRIA. The project also developed the interaction between *geographic addressing* and routing, and *wireless link characteristics and performance* as seen in Figure 1.3. The interactions between the other components are out of main focus of the dissertation.

Another key contribution is a cross-layer path selection decision algorithm. In VANET environments, existing access selection using wireless signal strength does not work well. Instead of wireless signal strength, we consider the use of geographic information for the path selection. In Figure 1.3, the path selection is performed based on the interaction with the three components providing the functions for *logical network routing*, *geographic addressing and routing*, and *wireless link characteristics and performance*.

Vehicle are equipped with multiple wireless network interfaces in order to connect to their communication peers from anywhere and at anytime. As addressed above, it is important to select appropriate interface to connect to the communication peers, however at the same time, there is also a demand to use multiple network interfaces simultaneously to increase network performance (ex. to increase total bandwidth). We introduce policy routing to enable the simultaneous usage of multiple paths.

The proposed contributions are implemented on Linux. Three different implementations of GeoNetworking have been used during this thesis: two of them were implemented by HITACHI Europe and NEC Europe under the framework of the GeoNet Project, and the other one was implemented by Espritec in collaboration with INRIA. We (INRIA) provided a sample code of the interface between *logical network routing* and *geographic addressing and routing* and we integrated it to all the implementations and led the validation of the all the implementations.

These implementations are tested and evaluated in both development environment and field operational testbed. For the evaluation performed with actual vehicles with realistic scenarios, we developed the evaluation tool named AnaVANET with collaboration in Universidad de Murcia.

We consider the key contributions of this dissertation to be:

- Proposing a scheme for combining IPv6 and GeoNetworking in order to take advantage of both IP and GeoNetworking. Unicast, multicast, anycast IP packets are encapsulated into the corresponding GeoNetworking specific communication types.
- Proposing a cross-layer path selection algorithm interacting with the three components providing *logical network routing*, *geographic addressing and routing*, and *wireless link characteristics and performance*.
- Defining the interface (Service Access Point (SAP)) between the cross-layer decision function and the network layer in conformance with the ISO/ETSI specifications.
- The interface between IP and GeoNetworking defined in the GeoNet project is implemented on Linux integrated in three distinct implementation of GeoNetworking and validated on a real field vehicular testbed. A performance evaluation of IPv6 GeoNetworking is performed.
- Designing and implementing the Service Access Point for IPv6 GeoNetworking. The specification of the Service Access Point defined in the GeoNet project is implemented on Linux based vehicle ITS Station. The implementation is tested and verified in real field testbed using vehicles. The network performance is measured in the testbed.
- Developing the AnaVANET evaluation and visualization tool to evaluate all types of vehicular networks in this dissertation. AnaVANET traces all data packets transmitted or forwarded by vehicles. It thus detects packet losses and can generate both end-to-end and per-hop statistics, as well as joint the metrics from link layer to transport layer and geographic metric such as speed, position and distance.

1.4 Overview of the Dissertation

This dissertation is organized as follows.

In **Chapter 2**, we present the terminology and the research and development activities related to cooperative ITS domain. We overview related standardization organizations and research programmes in Europe and worldwide. Among the standardization organizations, ISO, ETSI and IETF provide the most relevant standards for this study. The Framework Programme is the research plan led by the European Commission, and CVIS, GeoNet, ANEMONE, ITSSv6 and DriveC2X are key contributors to the domain of Cooperative ITS. The C2C-CC is an industry forum initially started by the European automotive manufactures. COMeSafety is an harmonization effort in order to consolidate the results of previous projects. The consolidation led to the specification of the ITS Station reference architecture and its later standardisation at ISO/ETSI. This study follows this architecture and terminology used in ISO/ETSI standards. There are four basic sub-system in the architecture (vehicle, roadside, central and personal ITS Stations), and cooperation of these ITS Stations achieve the common objective of cooperative ITS. To discuss the communication between the ITS Stations, three types of ITS communication modes are defined: Vehicle-based, Roadside-based and Internet-based ITS communication modes.

Chapter 3 provides an overview of all the possible technologies needed in cooperative ITS including network technologies and access technologies. First, physical layer and link layer for wireless technologies are summarized and then, various network protocols are explained. As network layer protocols, a taxonomy is proposed to divide the protocols mainly divided into infrastructure-less class and infrastructure-based class. The infrastructure-less class is known by the research area of MANET. As MANET routing protocols, topological routing and geographical routing are explained. Address auto-configuration mechanisms and in-vehicle Network Discovery are presented as a context of MANET. The infrastructure-based protocols are roughly classified into three categories: Internet mobility support, mobility enhancement and others. Internet mobility support is a set of technologies to allow mobile nodes' application to use a stable IP address as an Identifier while it also allows the packet routing with the other IP address as a Locater in the logical topology. We explain the key technology of the thesis, NEMO and the other mobility support technology. Mobility enhancement is a set of technologies used with the Internet mobility support to supply a better communication to mobile nodes.

In **Chapter 4**, we present issues and design requirement to optimize the communication between ITS Stations in IP-based cooperative ITS. First, three issues are presented. *Path selection* is a decision-making issue selecting an appropriate path matched with application requirements from the multiple paths exist between vehicle ITS Stations. The path selection process must be performed as the combination of the selections of various parameters (Communication Interface (CI), locator, Access Router (AR), routing and anchor). To allow intelligent path selection, geographic information plays an important role. *Geographic Position Management* is an issue about how to propagate and manage the geographic information in ITS Stations. To combine IPv6 and GeoNetworking, we are facing new *addressing and routing issues*. To realize IPv6 GeoNetworking, we must investigate how the IPv6 packets are delivered over GeoNetworking without *IPv6-awareness* in order not to impact too much the ITS Station reference architecture.

Then, we explain what are the design requirements for the solution. The solution shall follow the ITS Station architecture described in Section 2.2 keeping layers independence. The

parameters and messages exchanged between the layers must be flexible and be abstracted as much as possible for future extension. We follow the design concept of ITS Station router and host split where the ITS Station router is in charge of entire station communication and the hosts running applications are freed from the communication management. The IPv6 GeoNetworking solution must support all the new types of geographic routing communications (*e.g.* GeoBroadcast described in Section 3.3.2.2). To support IPv6 GeoNetworking, the GeoNetworking management should be transparent from the ITS Station host running applications. ITS Station must be able to change the point of attachment one link to another without interrupting the ongoing IP sessions. *i.e.* Network Mobility support is needed. The paths must be used according to the application requirements and multiple paths must be used simultaneously.

In **Chapter 5**, we present our approach in designing our solution to the problem expressed in the previous chapter, and in accordance with the design requirements. In order to optimize the communication between ITS Stations in IP-based cooperative ITS, we need to address the following six questions: What is the fundamental information required by the ITS Station Management Entity (SME), where the information comes from, which information is maintained in the network layer, how the network information is provided to the SME, how the path is selected and how IPv6 and GeoNetworking are combined. To answer these questions, we investigate how the network layer parameters are abstracted in the management entity and how the parameters are transmitted between the SME and the network layer. The investigation leads us to define three tables in the SME, the ITS Station information table, the path information table and the flow requirement table. We also figure out that four primitives are required for the interaction between the SME and the network layer. Two of them are needed to instruct the network layer to route flows to a given path and correspond to the primitives already defined in ISO specifications (*MN-REQUEST* and *MN-COMMAND*) for a network layer protocol block other than IPv6, whereas two new ones are needed to access to the information contained in the Management Information Bases (MIB) already defined in the network layer IPv6 protocol blocks. An adaptation agent is needed in the IPv6 protocol block in order to exchange the information with the SME and to process instructions coming from the SME. We then investigate how the best path is selected. The path selection decision is performed in the SME according to the application requirements recorded in the flow requirement table and the network status and interface information recorded in the path information table. It is important for intelligent path selection to predict the candidate path and its characteristics. The prediction performed in the SME is stored in the path information table. Finally, We investigate how IPv6 and GeoNetworking are combined. The IPv6 packets are encapsulated into GeoNetworking packets in the ITS Station router which is responsible for communication of the entire ITS Station and is managing GeoNetworking transparently to the ITS station hosts. A network-layer internal interface is needed to transmit packets between IPv6 and GeoNetworking (GeoIP SAP). As a result of this investigation, an abstraction model for management and network interaction is presented. Finally, we conclude this chapter by showing how the three major contributions *i.e.* the path selection manager, the interaction between the SME and the network layer (MN-SAP) and IPv6 GeoNetworking mechanisms are going to be presented in the following chapters.

In **Chapter 6**, we propose the cross-layer path selection decision-making module called path selection manager. Our main interest is to offer intelligent path selection decision to all

applications running on ITS Station hosts, while keeping the decision process independent from any specific network layer protocol. The decision process is divided into mainly two part: the inputs of abstracted network layer parameters from SAPs to the management parameters, and the output to the network layer protocol blocks based on the decision. First, we present three management parameters required for the decision-making: ITS Station information table, path information table and application requirement list. The ITS Station information table and the path information table are newly defined following the approaches from the result of the investigation in Chapter 5, whereas the application requirement list is extended from the one that has been defined in ISO. Then we introduce how the path is selected based on these management parameters. The path selection manager are further divided into path calculation phase and the decision-making phase. In the path calculation phase, the all the candidate paths are calculated based on the information about Communication Interface (CI), Topological Locator, Nexthop, Anchor, and Capabilities. Also in this phase, the availability of the paths are estimated based on various information. As an example, we present a geographical information based path availability estimation. The results of the candidate path calculation and the path availability estimation are stored in the path information table. In the decision-making phase, the Multiple Attribute Decision Making (MADM) method is employed in the path selection algorithm. The decisions are transmitted to the network layer.

In **Chapter 7**, we define the interface (MN-SAP) between the ITS Station Management Entity (SME) and the ITS Station Network and Transport layer (SNT) allowing the path selection manager in the SME to instruct the IPv6 protocol block in the SNT to route packets of a given flow to a given IPv6 path. Four primitives are required for the interaction between the SME and the SNT. First, we propose two new primitives (*MN-GET* and *MN-SET*) allowing the path selection manager to access to some of the parameters (*N-Parameters*) recorded in the existing Management Information Base (MIB) of the IPv6 and TCP/UDP protocol blocks in the SNT. The two other ones (*MN-REQUEST* and *MN-COMMAND*) are needed to instruct the IPv6 protocol block to route flows to a given path and correspond to the primitives already defined in ISO specifications for a network layer protocol block other than IPv6 (i.e. FAST). We thus extend these primitives to transfer the necessary information between the path selection manager and the IPv6, GeoNetworking and TCP/UDP protocol blocks of the SNT. We figure out that the current ISO specification of *MN-REQUEST* and *MN-COMMAND* commands do not fulfill our design requirements described in Chapter 4. Thus we define five new *MN-REQUEST* commands (*STAGeoNot*, *STATopoNot*, *STAServNot*, *PathNot*, and *PathMetricNot*) and three new *MN-COMMAND* commands (*STAServDiscov*, *PathMNG*, *FlowPolicy*) to accommodate our needs for path selection.

Then we explain how these commands are actually used. To do so, we first present the mapping between the abstracted parameters contained in the ITS station information, Path information and Flow requirement tables in the ITS station management entity and the corresponding parameters in the IPv6 and GeoNetworking protocol blocks of the ITS station network & transport layer. Then, to show the interaction between the management entity and the network layer, we describe the complete path selection procedure, from the activation of Communication Interfaces (CIs) to the transmission of flow policy instructions.

Note that this study is based on year 2011 versions of the ISO Standards and that the standards constantly evolve. As a result, primitives and parameters of the MN-SAP may have changed at the time of reading.

In **Chapter 8**, we present the mechanisms allowing the combination of IPv6 and GeoNet-

working according to the requirements expressed in Chapter 4. First, we review the functional modules and the interfaces between the entities composing the IPv6 GeoNetworking architecture as it was defined in the GeoNet Project. Following the approach presented in Chapter 5, the GeoNetworking module is defined as a sub-layer of IPv6. GeoNetworking therefore appears as an access layer and is presented to IPv6 in the form of a Communication Interface (CI) with GeoNetworking capabilities. The IPv6 packets delivered in a VANET where GeoNetworking is used as a multi-hop routing protocol are thus encapsulated into a GeoNetworking packet by the ITS Station router which is responsible for communication of the entire ITS Station and is managing GeoNetworking transparently to the ITS station hosts. An network layer internal interface is needed to transmit packets between IPv6 and GeoNetworking. We thus specify the GeoIP Service Access Point (GeoIP-SAP) between GeoNetworking and IPv6. In the GeoIP SAP, IPv6 packets are mapped to one of the four GeoNetworking communication types (e.g. *GeoUnicast*, *GeoBroadcast*) depending on the destination IP address. Finally, in order to alleviate the constraints that an IPv6 subnet is restricted to a geographic area, we propose the end based geographic link model. In the proposed link model, the IP address used to the roadside-based communication mode is determined by each vehicle ITS Station with more precise vehicle's information.

In **Chapter 9**, we present the software implementation of our system. All the modules are implemented in the ITS Station router runs the Linux operating system. We introduce Routing Policy Database (RPDB) for IPv6 routing in order to enable the simultaneous usage of multiple paths (*e.g.* vehicle-based, roadside-based and Internet-based), that is one of design requirements described in Chapter 4. Three different GeoNetworking implementations have been developed during this thesis: two of them were implemented under the framework of the GeoNet Project, and the other one was implemented by IMARA(France) and Espritec(Tunisia) collaboration team. We (INRIA) provided a sample code of GeoIP-SAP defined in Chapter 8 to all the implementations and led the validation of the all the implementations. The IPv6 packets are transmitted to the GeoNetworking module via TUN virtual interface. This virtual interface allows IPv6 to treat the GeoNetworking module as one of the Communication Interfaces (CIs) from IPv6 point of view. The path selection manager described in Chapter 6 was partially implemented as an extension of the open-source NEMO implementation (NEPL). The path availability estimation described in Chapter 6 is used to select the appropriate AR.

Implementation of simultaneous usage of multiple paths are published in [Tsukada2008, Tsukada2010a], and the details of the two IPv6 GeoNetworking implementations in the framework of the GeoNet project can be seen in [GeoNet-D.3, Tsukada2010b, Ines2010]. The other IPv6 GeoNetworking implementation is published as an open source CarGeo6 package [Toukabri2011].

In **Chapter 10**, we present our goals of the evaluation used for the performance evaluation presented in Chapter 11, 12 and 13. The first section describes the four major goals and the second section presents the methodology using an indoor test environment and an outdoor field test environment mad up to four vehicles. Details of the tests performed are presented in the following section.

The goals are to measure performance improvement thanks to simultaneous usage of multiple paths, the overhead using IPv6 GeoNetworking, the overhead using NEMO over IPv6 GeoNetworking and to analyze various affects of the conditions to the metrics. Then the network configuration, the vehicular platform, parameters, metrics (Round-Trip Time (RTT),

throughput, jitter, Packet Delivery Ratio (PDR), the number of hops) and experiment scenarios are described. We developed the packet analysis and visualization tool called AnaVANET in order to understand the affect of various condition to the metrics for outdoor test evaluation.

Chapter 11 shows the evaluations of MANEMO, *i.e.* the combination of MANET and NEMO offers a number of benefits, such as route optimization or multihoming. With the aim of assessing the benefits of this synergy, this chapter presents a policy-based solution to distribute traffic among multiple paths to improve the overall performance of a vehicular network. An integral vehicular communication testbed is developed to carry out field trials. First, the performance of the Optimized Link State Routing (OLSR) is evaluated in a vehicular ad-hoc network with up to four vehicles as a benchmark in order to compare with IPv6 GeoNetworking under the same conditions in the next chapter. AnaVANET is used to analyze the impact of the vehicles' position and movement on the network performances. Performance results have been geo-located using GPS information. Second, by switching from anchored path (NEMO path) and direct path (OLSR path), paths between vehicles are optimized and the final performance is improved in terms of latency and bandwidth. Our experimental results show that the network operation is further improved with simultaneous usage of NEMO and MANET.

Chapter 12 presents an experimental evaluation of IPv6 GeoNetworking stack implemented by HITACHI and by NEC in the GeoNet project (INRIA involved in the implementation of GeoIP SAP module described in Section 8.5).

We have conducted our experiments on both indoor testbed and outdoor testbed to evaluate the network performance on IPv6 GeoNetworking. The indoor test environment is designed to evaluate the pure performance of IPv6 over GeoNetworking avoiding interferences due to unexpected radio perturbations. We measured the network performance with UDP, TCP and ICMPv6 traffic using *iperf* and *ping6*. Considering the outdoor test, we can see that IPv6 over GeoNetworking works according to the specification in various driving scenarios. The communication is stable even when the vehicle speed is around 100 km/h and when the relative speed between vehicles is high. The radio range is much better than expected. The maximum distance of communication range is around 450 meters and it is not interrupted by the buildings on INRIA campus (all of them has only one floor). This calls for more field tests in urban environments.

In **Chapter 13**, we describe the evaluation results of performance measurement of the CarGeo6 implementation, by means of experimental evaluation in indoor testbed and outdoor testbed. The basic configuration of the evaluation is common with the test performed in the previous chapter using the GeoNet implementations. Thus we compare the performance difference between them. With outdoor testbed, we evaluate the performance in Internet-based communication by combining CarGeo6 and NEMO implementation (MIP6D). The performance measurement are processed and analyzed with AnaVANET.

More details of indoor tests are published in [Toukabri2011].

Part I

State of The Art

Chapter 2

Terminology and Context of This Study

Contents

In this chapter, we present the terminology and the research and development activities related to cooperative ITS domain. We overview related standardization organizations and research programmes in Europe and worldwide. Among the standardization organizations, ISO, ETSI and IETF provide the most relevant standards for this study. The Framework Programme is the research plan led by the European Commission, and CVIS, GeoNet, ANEMONE, ITSSv6 and DriveC2X are key contributors to the domain of Cooperative ITS. The C2C-CC is an industry forum initially started by the European automotive manufactures. COMeSafety is an harmonization effort in order to consolidate the results of previous projects. The consolidation led to the specification of the ITS Station reference architecture and its later standardisation at ISO/ETSI. This study follows this architecture and terminology used in ISO/ETSI standards. There are four basic sub-system in the architecture (vehicle, roadside, central and personal ITS Stations), and cooperation of these ITS Stations achieve the common objective of cooperative ITS. To discuss the communication between the ITS Stations, three types of ITS communication modes are defined: Vehicle-based, Roadside-based and Internet-based ITS communication modes.

2.1 Research and Standardization

In Europe, as shown in Figure 2.1, three main categories of organizations are interacting in ITS related activities (standardization organizations (SDO), European projects, ITS academic and industry forum). The European standardization organizations are collaborating with the world standardization organizations such as ISO, IETF, IEEE, ITU that are described in Section 2.1.1. The research and development is performed in European projects and national projects by the industries in Europe. The outcomes from ITS research and development are consolidated in COMeSafety [COMeSafety-final] and industry forums such as the C2C-CC[C2C-CC-Manifesto2007].

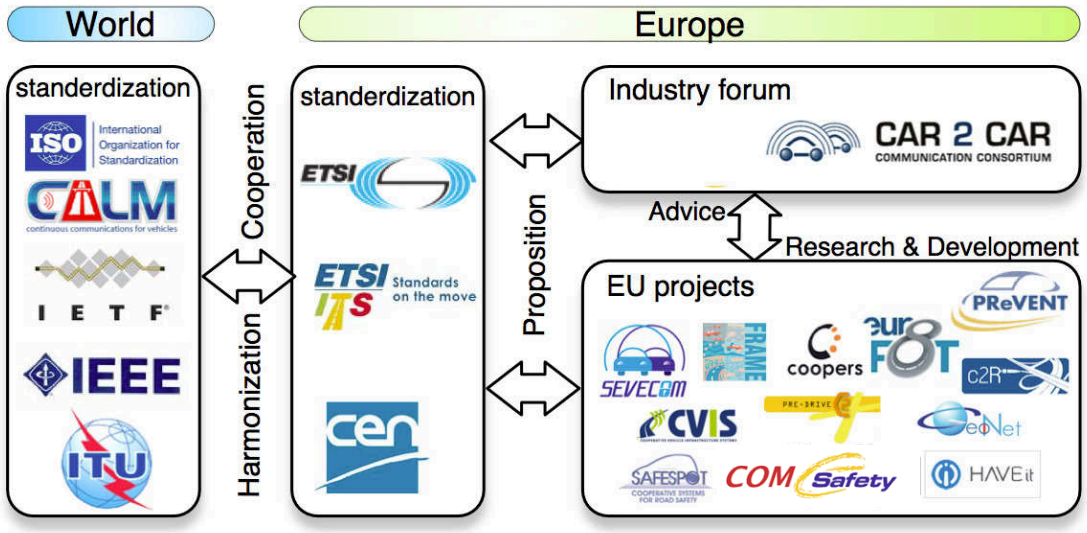


Figure 2.1: Overview of ITS activities in the world and Europe

2.1.1 Standardization Organizations (SDO)

2.1.1.1 ISO

The **International Organization for Standardization (ISO)** is a network of the national standards organizations of 161 countries, one member par country. ISO is a non-governmental organization that forms a bridge between the public and private sectors. The responsible technical committee for ITS is TC204. The working group 16 of TC204 called Communications Architecture for Land Mobile (CALM) is defining a communication architecture for cooperative ITS. The architecture covers all the layer of OSI reference model from the physical layer up to the application layer. All types of media (Wifi, IEEE802.11p (CALM M5), infrared, 2G, 3rd Generation mobile telecommunications (3G), Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WIMAX)) can be accommodated in the architecture. It allows both Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication modes. It covers all the range of communication (short, medium, long) and all types of the applications *i.e.* road safety, traffic efficiency, comfort and infortainment. IPv6 and non-IP (FAST) are possible protocols at the network layer.

2.1.1.2 ETSI

The **European Telecommunications Standards Institute (ETSI)** is the standardization organization for ICT in Europe. ETSI has more than 700 member organizations from over 60 countries in the world. The responsible technical committee for ITS is ETSI TC ITS. Since 2009, ISO TC204 WG16 and ETSI TC ITS have converged towards the ITS Station reference architecture detailed in Section 2.2.

2.1.1.3 IEEE and WAVE architecture

The **Institute of Electrical and Electronics Engineers (IEEE)** is the leading professional association for advanced technologies. The scope of IEEE was originally electrical electronics engineering, and today, it expands into many related fields. The standards of the organization from IEEE are, for example, Bluetooth is defined as IEEE802.15.1, Wireless LAN is defined as IEEE802.11a/b/g and the IEEE802.11 variant for vehicular communication is defined as IEEE802.11p.

The IEEE 1609 family of standards for Wireless Access in Vehicular Environments (WAVE)[1] defines an architecture illustrated in Figure 2.2. It defines a standardized set of services and interfaces that collectively enable secure V2V and V2I wireless communications. IEEE 1609 Standards and the other standards are illustrated with different colors in Figure 2.2.

[IEEE-1609.0-Arch] describes the WAVE architecture shown in Figure 2.2 and services necessary for multi-channel DSRC/WAVE devices to communicate in a mobile vehicular environment. As the two columns in Figure 2.2 shows, the architecture has OSI like stack in data plane and vertically connected Management plain as well as the ITS Station architecture in Section 2.2. There are two main cases such as using TCP/UDP/IPv6 to support existing applications and using WAVE Short Message Protocol (WSMP) to support WAVE applications.

As WAVE applications, or to support WAVE applications, Remote Management Services, Over-the-Air Electronic Payment Data Exchange Protocol and Dedicated Short Range Communications (DSRC) Message Set Dictionary are specified. Remote Management Services

[1] http://vii.path.berkeley.edu/1609_wave/

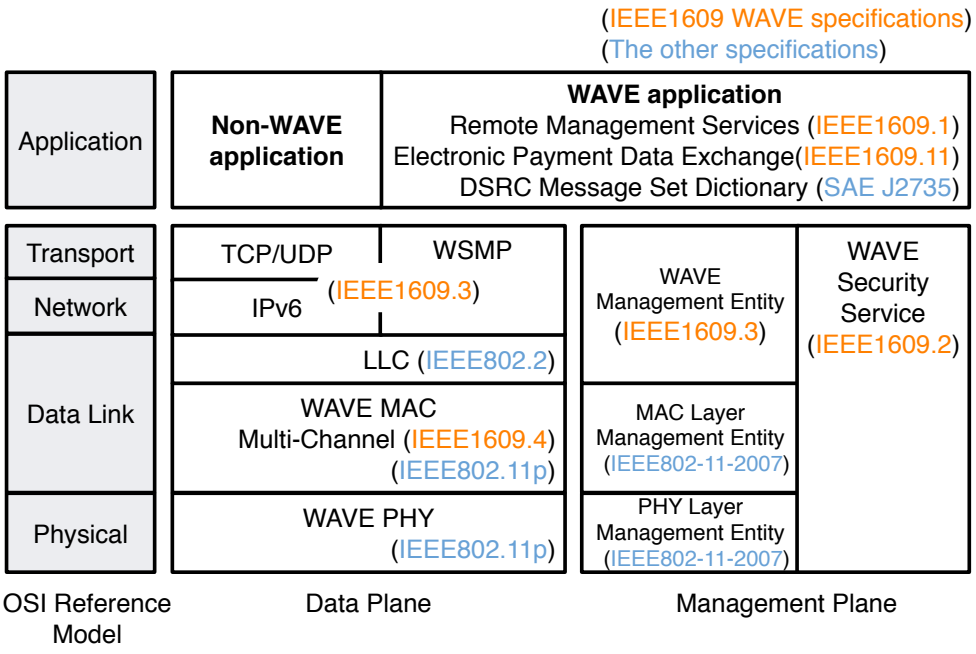


Figure 2.2: WAVE architecture

[IEEE-1609.1-RemoteMNG] is designed to allow applications at remote sites to communicate with On-Board Units (OBUs) through Road Side Units (RSUs). It acts as an application layer and conducts information interchange, needed to implement the requirements of the remote WAVE applications. Over-the-Air Electronic Payment Data Exchange Protocol [IEEE-1609.11-Payment] is the electronic payment service layer and profile for Payment and Identity authentication, and Payment Data transfer for WAVE applications using roadside-based communication. DSRC Message Set Dictionary [SAE-J2735-DSRC-Message-Set] defines a message set, and its data frames and data elements specifically for use by WAVE applications.

Layer 3 and 4 of the OSI model in the WAVE architecture [IEEE-1609.3-Networking] employs IPv6, TCP and UDP elements of Internet model. Beside these elements, WSMP is defined to support WAVE applications. Management and data services within WAVE devices are provided.

In Datalink layer, Logical Link Control (LLC) sublayer [IEEE-802.2-LLC] and WAVE Medium Access Control (MAC) is used. WAVE MAC basically follows the specification of IEEE 802.11p [IEEE802-11p], but with multi-channel operations [IEEE-1609.4-MultiChannel] including the operation of control channel (CCH) and service channel (SCH) interval timers, parameters for priority access, channel switching and routing, management services, and primitives designed for multi-channel operations.

In Management Plane, secure message formats, and the processing of those secure messages, within the WAVE system are defined in [IEEE-1609.2-Security]. The standard covers methods for securing WAVE management messages and application messages, with the exception of vehicle-originating safety messages. It also describes administrative functions necessary to support the core security functions. MAC Layer Management Entity (MLME) and PHY Layer Management Entity (PLME) in the Management plane interact with MAC and Physical (PHY) in Data plane via MLME and PLME SAPs defined in [IEEE802-11-2007]

in order to exchange cross layer information.

2.1.1.4 IETF

The technologies related with Internet are discussed and standardized in the **Internet Engineering Task Force (IETF)**. The organization is international and open for every one such as network designers, operators and researchers. Different topics are discussed in working groups and any one can follow the discussion.

ITS related working groups are illustrated in Figure 2.3. Mobile IP [rfc6275, rfc5944] (see details in Section 3.4.1), *mip4* Working Group (WG) is working on Mobile IPv4, *mip6*WG is discussed about Mobile IPv6. In past, NEMO was discussed in *nemo* WG and multihoming for NEMO and Mobile IPv6 was discussed in *monami6* WG. *Mip6*, *nemo*, and *monami6* are merged into *mext* WG in 2007. *Mipshop* is the working group that discusses for improvement of signaling of mobility support. In addition, to discuss about Proxy Mobile IP, *netlmm* WG was setup in 2006 and *netext* WG was created to investigate more advanced feature of Proxy Mobile IP.

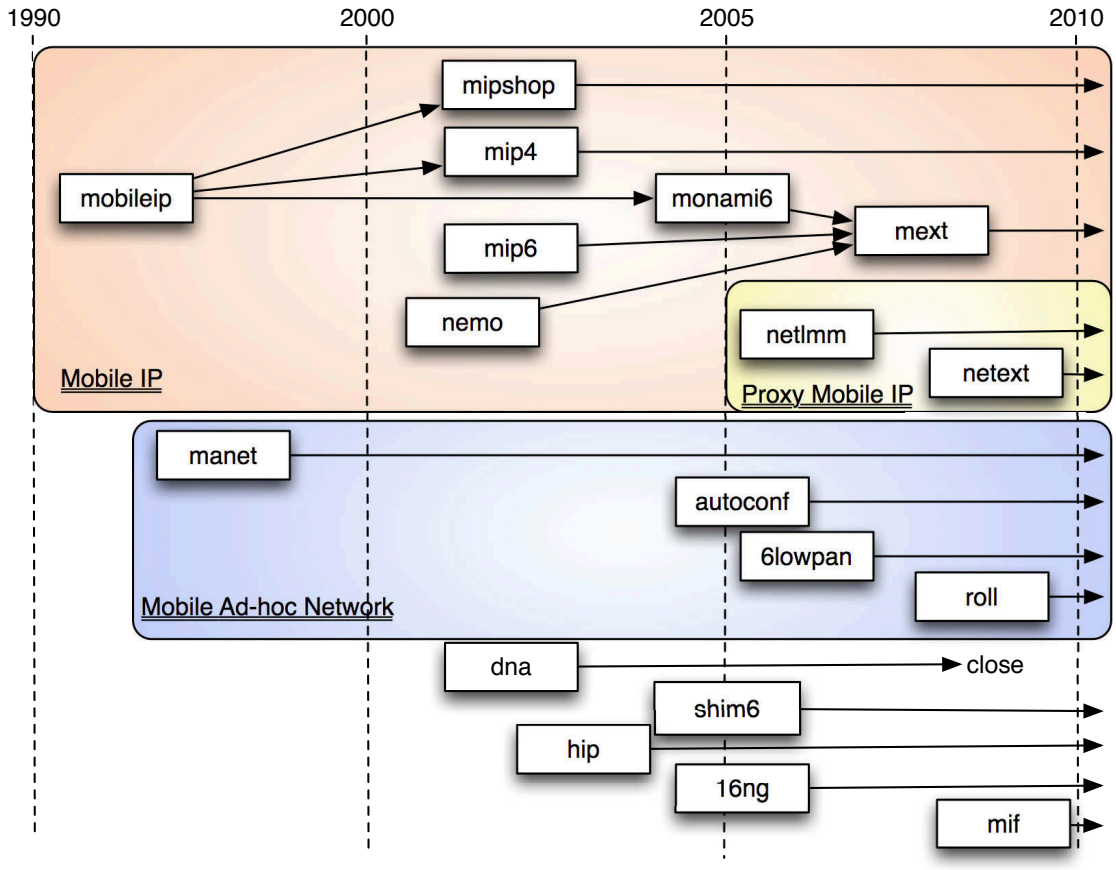


Figure 2.3: IETF activities related to ITS

For discussing MANET used for V2V, *manet* WG has a long history since 1997. Auto-configuration in MANET is discussed in *autoconf* WG. The low power personal area net work are investigated in *6lowpan* WG, and the low power sensor networks are discussed in

roll WG. The other WGs that are related to ITS is *shim6* WG that treats site multihoming, *mif* WG that works on multiple network interfaces usage, *16ng* WG discuss for IPv6 over IEEE802.16 or WIMAX and *hip* WG investigate Host Identity Protocol (HIP). *dna* WG that worked on Detecting Network Attachment is also related in ITS.

2.1.1.5 Other Standardization Organizations

The **International Telecommunication Union (ITU)** is an agency of the United Nations which regulates information and communication technology issues. ITU has coordinated the shared global use of the radio spectrum, promoted international cooperation in assigning satellite orbits, worked to improve telecommunication infrastructure in the developing world, established the worldwide standards.

The **European Committee for Standardization (CEN)** is a business facilitator in Europe, removing trade barriers for European industry and consumers. Its mission is to foster the European economy in global trading, the welfare of European citizens and the environment. The ITS related topics are discussed in CEN TC 278.

2.1.2 The European ICT Research

In 2006, the Intelligent Car Initiative was created in order to improve the efficiency of transportation systems using ICT [Intelligent-Car-Initiative2006]. The initiative is "*one of the 3 Flagship initiatives proposed within the third pillar with the objective to raise the visibility of the vital contribution of* ICT *to the quality of life*". The initiative manages the eSafety forum created by the European Commission for the cooperation among industrial association, companies, public sector and all the stockholders related to transportation[eSafety2003]. The COMeSafety project was funded as Sixth Framework Programme (FP6) Specific Support Action (SSA) to supports the eSafety Forum with respect to all issues related to V2V and V2I communications as the basis for Cooperative ITS.

The Framework Programme is the research plan led by the European Commission in order to support and encourage research in Europe since 1984. The FP6 took place from 2002 until 2006 and the Seventh Framework Programme (FP7) is taking place from 2007 to 2013. The funding of FP6 was 17.9 billion euros for 4 years [Funding-FP6] and the 50.5 billion euros for FP7 for 7 years [Funding-FP7]. The ICT sector always had the most budget share since the Second Framework Programme. In FP6 , 3.9 billion euros are funded to ICT sector, which represents 21% and in FP7, 9 billion euros are allocated to ICT sector that is about 19% of total FP7 funding. The funding in FP6 and FP7 are summarized in Table 2.1.

	All the sectors		ICT sector	
	All period	A year	All period	A year
FP6 (4 years)	€ 17.9 billion	€ 4.4 billion	€ 3.9 billion	€ 1.0 billion
FP7 (7 years)	€ 50.5 billion	€ 7 billion	€ 9 billion	€ 1.3 billion

Table 2.1: Budget of Framework Programme

ITS related FP6 and FP7 projects are listed in Appendix A and Appendix B, respectively. The FP6 had 45 ITS related project and 381.7 million euros were allocated to these projects. The biggest projects were Prevent (54 million euros), CVIS (41 million euros), Safespot (38 million euros) and Coopers (16.8 million euros). On the other hand, FP7 has not been concluded yet, and it already allocated 184.2 millions euros to the ITS related projects until

June 2010. The biggest project is HAVE-IT (28 million euros), teleFOT (14 million euros) and euroFOT (14 million euros).

2.1.2.1 GeoNet Project

Period: February 2008 - February 2010
Budget: 3M euros
Partners: 7 organizations, 6 countries

To increase the road safety in Europe while traffic and driver's concentration demand also rises, the EC and the automotive industry have committed to halve the life loss by 2010. The GeoNet project will significantly contribute to this goal by implementing a reference specification of a geographic addressing and routing protocol with support for IPv6 to be used to deliver safety messages between cars but also between cars and the roadside infrastructure within a designated destination area.

While the Car-to-Car Communication Consortium (C2C-CC) (detailed in Section 2.1.3) has invested significant effort into the specification of a car-to-car communications mechanism suitable for safety applications, its mandate does not extend beyond defining a specification. At the same time, ongoing projects like SafeSpot would need an actual implementation to rely on whereas other such as CVIS are developing a communication architecture relying on the maintenance of a constant access to the Internet over IPv6.

2.1.2.2 ITSSv6 Project

Period: February 2011 - February 2014
Budget: 2.5M euros
Partners: 7 organizations, 5 countries

ITSSv6 aims at developing a reference open-source IPv6 ITS Station stack available to European and national third parties using IPv6 for Internet-based communications in Field Operational Tests (FOTs) of Cooperative Systems. It provides an enhanced IPv6 ITS Station stack adapted to operational use in large scale FOTs based on the ITS reference architecture detailed in Section 2.2. The new software is validated on a basic open platform with recommended physical interfaces (802.11p and 3G). The project gathers key partners from the CVIS and GeoNet projects (See Section 2.1.2.1 for more details) and key expertise in the specification and development of the IPv6 software.

2.1.3 C2C-CC and C2C-CC Architecture

The Car-to-Car Communication Consortium (C2C-CC) [2] is a non-profit organization started by the European automotive manufactures, that is open to all the suppliers, research institutes, and other partners having interest in vehicle-to-vehicle communications in Europe. The objective is to improve the road safety and traffic efficiency by inter-vehicle communication. C2C-CC will publishes and develops an open European standard of ITS cooperative systems and the related verification process. C2C-CC contributes for standardization organizations to

[2] http://www.car-2-car.org/

make an European standards, and submits the specification to standardization organizations, especially ETSI TC ITS. C2C-CC pushes the standard to the worldwide standardization organizations with harmonization. As a manifesto, C2C-CC described the scenarios, the system architecture, and applications in [C2C-CC-Manifesto2007].

The C2C-CC architecture is the architecture proposed in C2C-CC to support active safety, traffic efficiency and infotainment applications [C2C-CC-Manifesto2007, GeoNet-D.1]. As vertically illustrated in Figure 2.4, three main scenarios are expected.

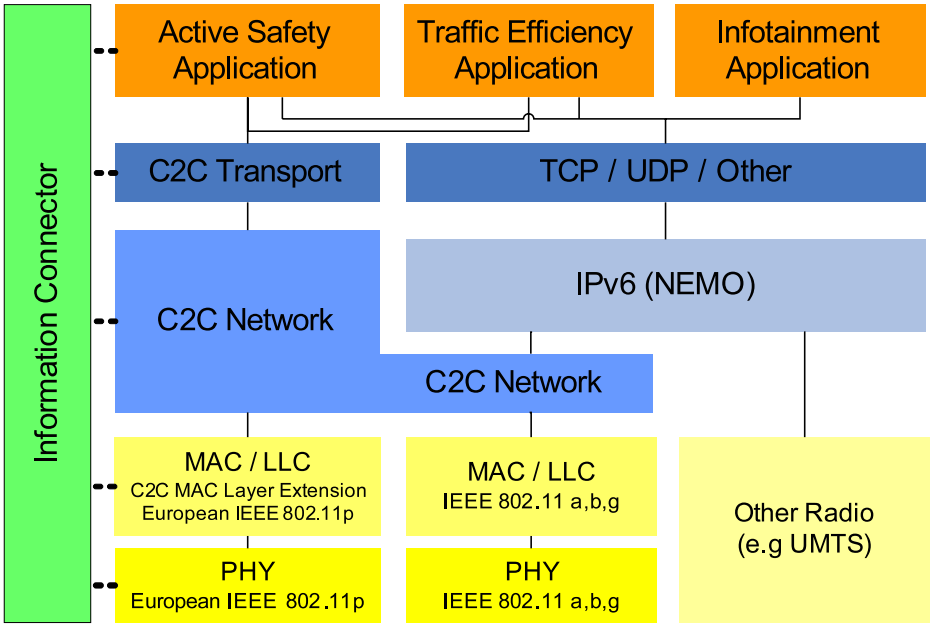


Figure 2.4: C2C-CC and GeoNet Architecture

The left most column is the scenarios that the Car-to-Car Network (C2CNet) (geographic routing and addressing protocol) is used as network layer protocol block and C2C transport is used as transport layer. In this case the underlying layer is modified version of IEEE802.11p [IEEE802-11p]. This mainly supports active safety applications and traffic efficiency applications.

On the other hand, the right most column is similar concept with the current Internet. It uses IPv6 network with supporting mobility using NEMO basic support described in Section 3.4.2. Pre-existing transport protocol blocks are used as transport layer such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

The middle column is the combination with the left most and right most columns. The protocols stack is designed to use both C2CNet and IPv6 at the same time as network layer protocol blocks. The key point is the interaction between the protocol blocks. The interface between C2CNet and IPv6 has been specified in the context of the GeoNet European project.

2.1.4 COMeSafety

COMeSafety is an harmonization effort, in order to consolidate the results of previous projects as shown in Figure 2.5 that is taken from the COMeSafety website[3]. It notably published an ITS communication architecture, taking into consideration results of CVIS, GeoNet, Prevent,

[3]COMeSafety: approach: http://www.comesafety.org/index.php?id=23

ISO Standards and C2C-CC work. The ETSI/ISO ITS Station reference architecture and the initiation of ETSI TC ITS is based on this ITS communication architecture. The final report of COMeSafety was published in February 2010 [COMeSafety-final]. From December 2010, COMeSafety2 continues coordinating the work in European standardization at ETSI and CEN. COMeSafety2 also focus on the cooperation with the United States and it includes one work package that is directly dedicated to the EU-US cooperation.

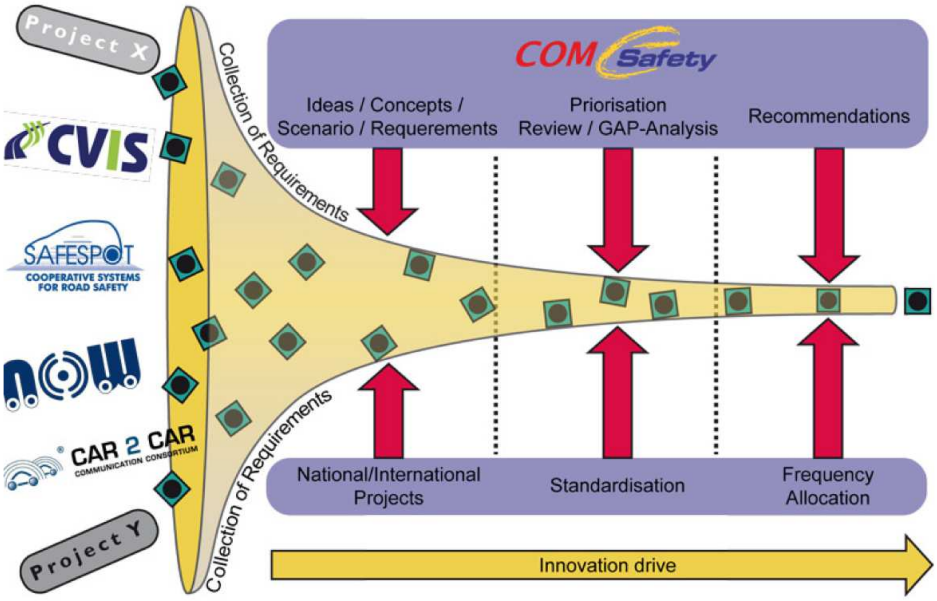


Figure 2.5: Approach of COMeSafety

2.2 ITS Station Reference Architecture

In the section, we present the ITS Station architecture [ISO-21217-CALM-Arch, ETSI-EN-302-665-Arch] specified by ISO and ETSI. The architecture reflects a consensus of the past work from ISO, ETSI, C2C-CC, GeoNet, COMeSafety and other projects presented earlier in this chapter.

2.2.1 ITS Station Architecture

Figure 2.6 shows the ITS Station architecture specified in ISO and ETSI. The graphical representations partly follow the ISO's OSI principle of separation of layers.

The ITS architecture consists of six main parts. In the data plane (middle of the figure), the ITS Station architecture has four layers that perform different tasks. From the bottom to the top, Access, Network & transport, Facilities and Application layers are stacked. The layers next to each other are connected via a Service Access Point (SAP). The management entity and security entity (both side of the figure) are connected to all the layer via the SAPs.

The access technologies layer [ISO-21218:2008-CALM-Medium-SAP] reflects CALM's objective to allow seamless communication over several coexisting radio access technologies. The architecture therefore includes mechanisms to dynamically select the most appropriate CI *i.e.* wireless interfaces and wired to be used. The management entity accesses to a CI via a Virtual Communication Interface (VCI) that provides a quick and efficient method to set the properties of a CI on a packet-by-packet basis without the continuous involvement of the

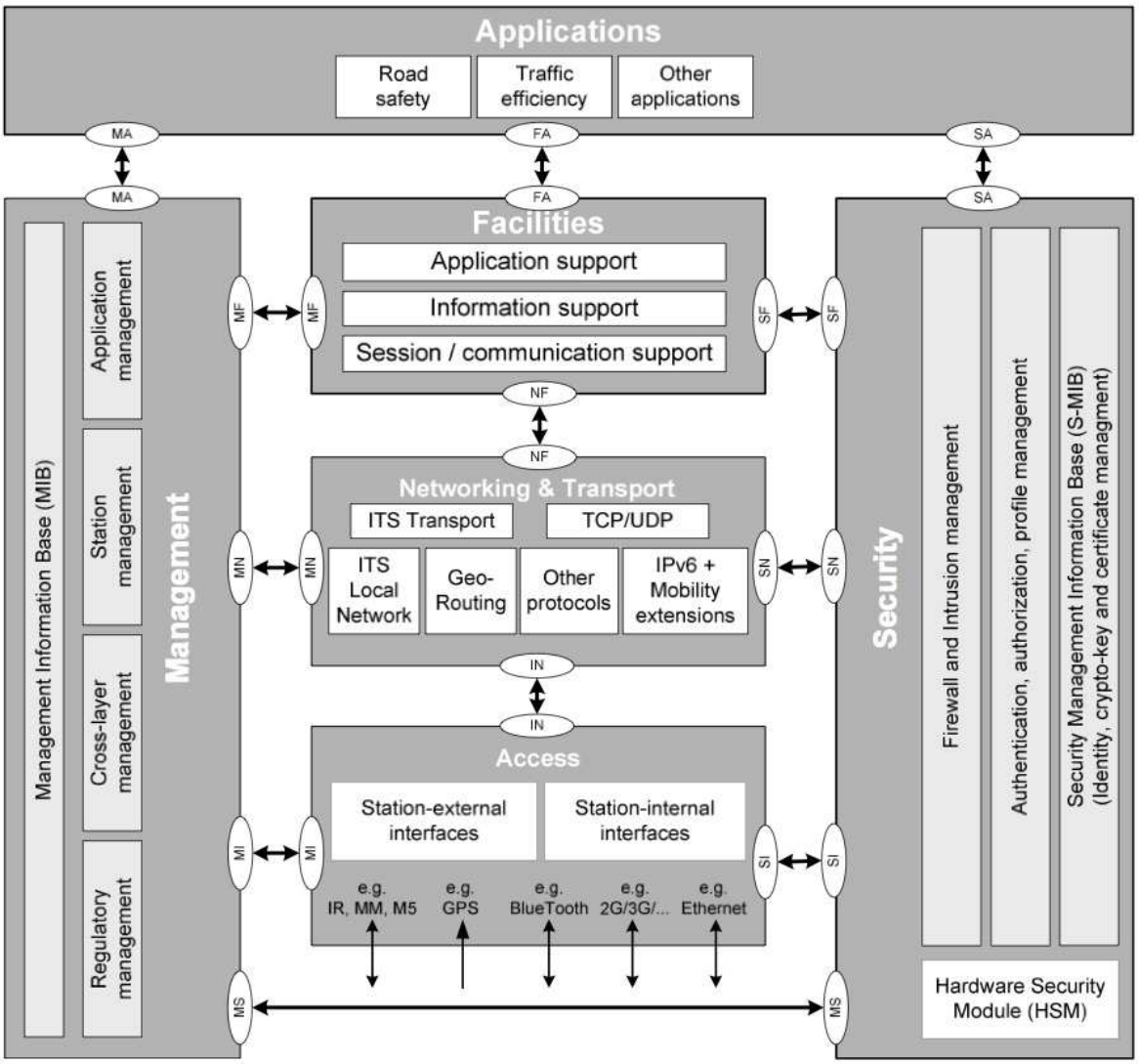


Figure 2.6: ITS station architecture

other entities. MI-SAP, IN-SAP and SI-SAP are defined to access the access technology layer from Management, Network/Transport and Security layer, respectively. Currently, 2G/3G, IEEE802.11p(ISO CALM M5 and ETSI G5), DSRC, millimeter wave, infrared, WIMAX, satellite and Ethernet are supported. Any other technology can be supported as long as it is adapt to the ITS Station reference architecture (*i.e.* SAP must be supported).

The Networking & Transport layer contains the different networking and transport protocol blocks needed for a fully functional communication in an ITS communication mode. As network protocol block, ITS Network, geographic routing, and IPv6 and other protocol blocks are used. IPv6 networking and non-IP networking are specified as standard in [ISO-21210:2011-CALM-IPv6] and [ISO-29281-CALM-non-IP], respectively, while GeoNetworking is specified in [ETSI-TS-102-636-3-GeoNetworking-Arch, ETSI-TS-102-636-6-1-IPv6-GeoNetworking]. GeoNetworking allows for multi-hop communication in a Vehicular Ad-hoc Network (VANET). GeoNetworking is detailed in the documents shown in Table 2.2. GeoNetworking is a network and transport layer protocol block used for vehicle-based communication and roadside-based

communication in order to meet ITS safety application requirements. Safety message requires secure, reliable, low-latency communication. The routing is based on geographic position of vehicles and roadside ITS Station, and supports not only point-to-point communication but point-to-multipoint communications where packets are distributed in a given geographic area. Upper layer of GeoNetworking can be Basic Transport Protocol (BTP) described in [ETSI-TS-102-636-5-1-Transport], and also IPv6 (and TCP/UDP). The later case is especially called IPv6 GeoNetworking and is one of the focus of the thesis.

To support mobility to a number of nodes in the vehicle, NEMO is used in IPv6 module. Each networking protocol block may be connected to a specific dedicated ITS transport protocol block or to existing transport layer protocol blocks, e.g. UDP, TCP. IN-SAP, MN-SAP, NF-SAP and SI-SAP are defined as interfaces from Access layer, management entity, Facility layer and Security entity, respectively.

#	Document	Contents
1	[ETSI-TS-102-636-1-req]	Requirements
2	[ETSI-TS-102-636-2-Scenario]	Scenarios
3	[ETSI-TS-102-636-3-GeoNetworking-Arch]	Network architecture
4.1	[ETSI-TS-102-636-4-1-Media]	Media-Independent Functionality
4.2	[ETSI-TS-102-636-4-2-Media]	Media-Dependent Functionalities for ITS-G5A media
5	[ETSI-TS-102-636-5-1-Transport]	Basic Transport Protocol
6	[ETSI-TS-102-636-6-1-IPv6-GeoNetworking]	IPv6 GeoNetworking

Table 2.2: GeoNetworking documents in ETSI

The Facilities layer provides a set of common functionalities which are shared by several applications for various tasks. The facilities provide data structures to store, process and maintain data of different type and source. Facilities can be classified into "*Application Support*", "*Information Support*" and "*Communication Support*" facilities. The Applications layer contains the user applications exploiting the communication functionalities provided by the remaining part of the communication protocol stack. "*Road Safety*", "*Traffic Efficiency*", and "*Comfort/multimedia*" are defined. As interfaces from Network/Transport, Management, Application and Security layer, NF-SAP, MF-SAP, FA-SAP and SF-SAP are defined. ETSI has specified three functionalities in the facilities layer:

Local Dynamic Map (LDM) A key facility element which supports various ITS applications by maintaining the information on objects influencing or being part of traffic [ETSI-TR-102-863-LDM].

Co-operative Awareness Messages (CAM) Messages distributed within the ITS-G5 (802.11p) network and provide information of presence, positions as well as basic status of communicating ITS stations to neighbouring ITS stations that are located within a single hop distance [ETSI-TS-102-637-2-CAM].

Decentralized environmental Notification Messages (DENM) Messages mainly used by the Cooperative Road Hazard Warning (RHW) application in order to alert road users of the detected events [ETSI-TS-102-637-3-DENM].

Service Advertisement Message (SAM) This message is designed for single-hop communications. It distinguishes a session initialization phase and a session operation phase. The concept is validated in the CVIS project. [ISO-24102-4-FSAP]

The management entity is a vertical plane handling cross-layer information exchange among the horizontal layers. The specification is standardized as [ISO-24102-CALM-Management]. The functionalities implemented in this entity include the dynamic selection of the access technology for a given application, the monitoring of communication interfaces' parameters, the management of transmission permissions and priorities, the management of services, the congestion control mechanisms and remote and local management. Layer information is exchanged with the ITS management entity via MN/MF/MI-SAPs.

Finally, the Security entity is the block implementing security services for the communication protocol stack and the management entity. The entity is connected to all the layers including Firewall/intrusion management, Authentication/authorization/profile management and Security management information base.

The ITS Station architecture is a result of discussion and consensus of various stakeholders in the ITS domain. The development of the ITS Station architecture will continue progressively with feedback from Field Operational Test (FOT). Success of business in cooperative ITS will drive active development of truly innovative software from many vendors on the market in the future. In the span of long-term ITS Station development, current technologies, such as GeoNetworking and NEMO or even IP itself, may be obsoleted by newer and better technologies at all the layers. Accordingly, some components at the architecture will be replaced by more intelligent ones as the demand of communication for cooperative ITS changes.

Standardization aims at accelerating the development by enforcing the interoperability between products from different venders. With open standards, a product on the market can be easily replaced by another product.

The ITS Station architecture enforces the interoperability inside the ITS Station as well as between different ITS Stations. The implementation of a module that follows the ITS Station architecture can be replaced by other implementation. For example, a more intelligent decision module can perfectly replace the previous decision module in the management entity thanks to the open architecture of ITS Station and standardized interfaces (SAPs) with the other layers. The progressive replacement by more intelligent software should accelerate the development of cooperative ITS.

2.2.2 Terminology

As we saw in Section 2.2.3, several organizations in Cooperative ITS domain share the basic ITS scenarios. However the terminology is slightly different each other. Table 2.3 summarizes the terminology used in ISO [ISO-21217-CALM-Arch]/ETSI [ETSI-EN-302-665-Arch], IETF [rfc6275, rfc3963], COMeSafety [COMeSafety-final] and C2C-CC [C2C-CC-Manifesto2007]/ GeoNet project [GeoNet-D.1].

In the first row, ISO/ETSI terminology emphasizes the ITS Station reference architecture explained in Section 2.2. IETF defines the IP layer functionality of each node as shown in the second row in Table 2.3. The terminology of COMeSafety is based on the role of the components, which distinguishes host and router by the role of communication and application as shown in the third row of Table 2.3 (Communication and Control Unit (CCU) and Application Unit (AU)). As shown in the last row of Table 2.3, the terminology of C2C-CC and GeoNet project focuses more on the place where the node is installed (On-Board Unit (OBU), Road Side Unit (RSU) and AU).

From now on, the rest of the dissertation combines the terminologies of ISO/ETSI and IETF, because ISO/ETSI terminology is important to to discuss ITS specificities whereas

the IETF terminology is needed to discuss about IP layer protocols since the dissertation mainly focuses on the network layer.

ISO / ETSI [ISO-21217-CALM-Arch, ETSI-EN-302-665-Arch]	IETF [rfc6275, rfc3963]	COMeSafety [COMeSafety-final]	C2C-CC/GeoNet [C2C-CC-Manifesto2007, GeoNet-D.1]
—	Mobile Node (MN)	—	—
ITS Station router	Mobile Router (MR)	Vehicle CCU	On-Board Unit (OBU)
ITS Station host	Mobile Network Node (MNN)	Vehicle AU	Application Unit (AU)
ITS Station router	Access Router (AR)	Roadside CCU	Road Side Unit (RSU)
ITS Station host	Correspondent node (CN)	Central AU	Correspondent AU
Home Agent (HA)	Home Agent (HA)	Home Agent (HA)	Home Agent (HA)

Table 2.3: Terminologies in the organizations

First, in the ITS communication modes, four main system components, which can communicate with one another are described, that are Vehicle ITS Station, Roadside ITS Station, Central ITS Station and Personal ITS Station. Seconds, the function of communication and application are separated into a router and hosts in ITS Station. ITS Station has at least one router to control the communication functions of the ITS Station. And in the ITS Station, hosts runs road safety, traffic efficiency, comfort and infortainment applications. However the function of the router and the host can be installed in a single node as it is an implementation choice.

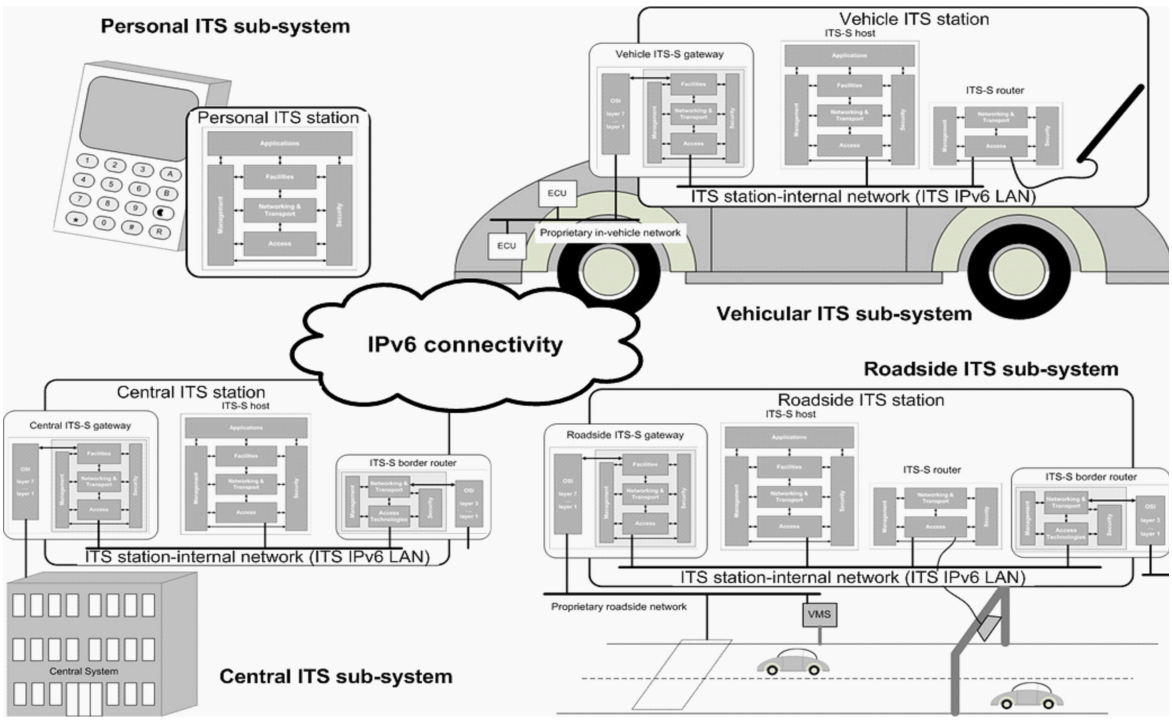


Figure 2.7: ITS sub-systems

Figure 2.7 gives ITS sub-systems found in [ISO-21217-CALM-Arch]. There are four main ITS sub-systems as follows:

- **Vehicle ITS Station**
  Vehicle ITS Station consists of two sub-components. A vehicle ITS Station router is in charge of communication with other vehicles or with Roadside ITS Station router. One or more vehicle ITS Station hosts run ITS applications in the vehicle. When ITS Station needs the information from the in-vehicle network, a Vehicle Gateway can be an interface between ITS Station and the in-vehicle network (e.g., CAN bus)).

- **Roadside ITS Station**
  Roadside ITS Station has two sub-components. A roadside ITS Station router is responsible for communication with vehicle ITS Station or with other Roadside ITS Stations. One or several road ITS Station routers run ITS applications. A Roadside Gateway provides an interface to access to legacy roadside infrastructure systems (e.g. Variable Message Signs (VMS))

- **Central ITS Station**
  Central ITS Station is the ITS Station fixed in a core network providing ITS Services. Central ITS has one or more ITS Station hosts that run ITS application. The application may collect the information from vehicle ITS Station or from roadside ITS via a Central Gateway.

- **Personal ITS Station**
  Personal ITS Station are nomadic devices carried by passengers, pedestrians or cyclists (*e.g.* PDA, smartphone). It consists of two main sub-components. Personal ITS Station router is in charge of communication with vehicle ITS Station or with roadside ITS Station. Personal ITS Station host runs ITS application. Both of personal ITS Station router and personal ITS Station host can be installed in a personal device.

Figure 2.8 illustrates the terminology used in the dissertation. ITS Station is the basic component of ITS and is fixed along roadside or installed in vehicle. ITS Station has both ITS Station router that maintains communication between the other ITS Stations and ITS Station hosts that run the various applications in the ITS Station.

ITS Station router controls the communication of the station and connects both vehicular ad-hoc domain and infrastructure domain. In vehicular ad-hoc domain, IEEE802.11p[IEEE802-11p] is used to connect between ITS Station routers. An ITS Station router fixed along the roadside connects to the infrastructure domain with wired network interface (i.e Ethernet). An ITS Station router installed in a vehicle can be connected to the Internet with cellular networks, WIMAX, etc.

A vehicle ITS Station is connected to the Internet in mobile environment. To enable network mobility support, a vehicle ITS Station router supports mobility. The vehicle ITS Station router that supports mobility is called as Mobile Router (MR).

The ITS Station host which connects to in-vehicles network behind of MR is Mobile Network Node (MNN). MNN can be portable device brought by passengers or built-in device in the vehicles. AR is the infrastructure side of point of attachment that provides Internet connectivity to the MR. The node in the Internet and make communication with vehicle ITS Station station is called as Correspondent Node (CN).

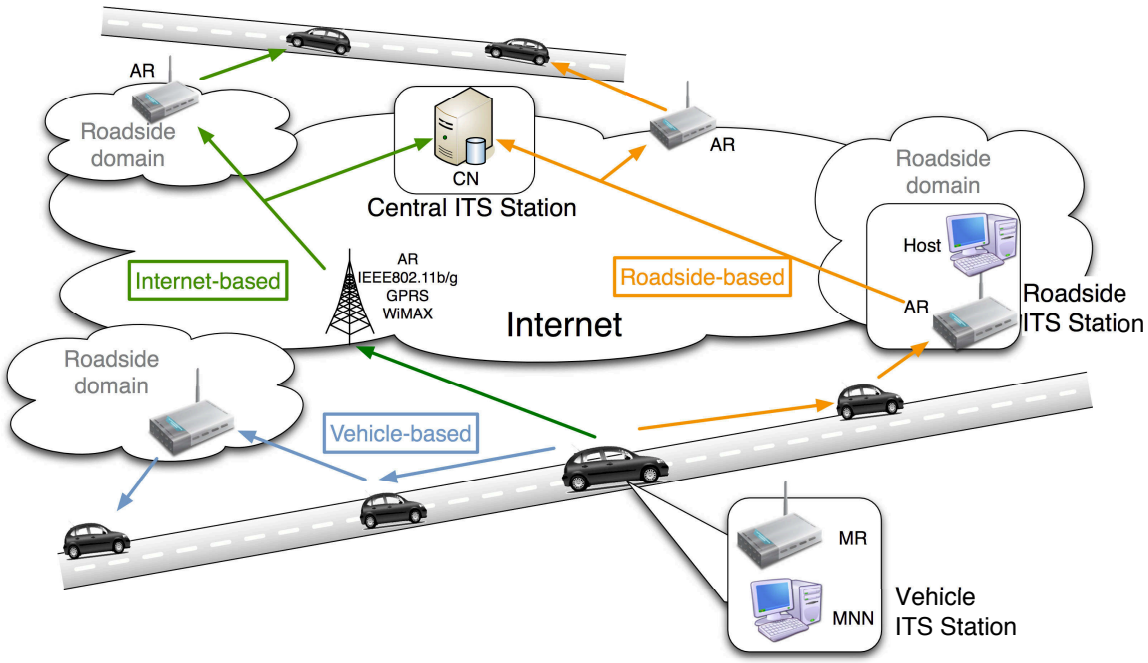


Figure 2.8: Terminology and ITS communication modes

2.2.3 ITS Communication Modes

In Cooperative ITS research, the terms of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) have been used to define the communication modes from historical reason. V2V means the communication without depending on any third-party infrastructure and V2I means the communication that some infrastructure involves. However, we found that this terminology is problematic to define the communication modes for this study.

First of all, the terminology has been understood by two different ways depending on which layer is mentioned. Regarding Layer 2 (L2), V2I stands for type of communication where mobile nodes communicate with one or more fixed infrastructure already deployed in the network in centralized mode. V2V stands for the type of communication where mobile nodes communicate without any infrastructure in ad-hoc mode, and in which they connect directly each other when they are within the radio range, or connect by multi-hop communication by some packet routing when they are not close each other.

On the other hand, regarding Layer 3 (L3) or upper than L3, V2I is understood as the type of communication where the data sent from a vehicle to a fixed infrastructure. In this case, the fixed infrastructure actually means the Internet and the term of V2I is used to discuss about the Internet connectivity of a vehicle supported by mobility technology such as NEMO to solve the mobility issues. Regarding L3 or upper than L3, V2V is the type of communication that the data exchanged between vehicles without depending on any infrastructure by using MANET.

IEEE802.11p [IEEE802-11p] that is designed for VANET does not have centralized mode. Thus ad-hoc mode is used for both V2I and V2V case in order to enable the multi-hop communication. Indeed, there is no difference between vehicle and infrastructure from wireless configuration point of view. Thus the distinction between V2I and V2V is not useful in L2, because L2 point of view, an infrastructure is considered as a fixed vehicle which is connected to the Internet with wired access.

In L3, which is main focus of the study, the previous definition of V2I and V2V is also not clear, because only both end nodes of the communication cannot classify the communication modes. For example, when V2I is defined as the communication between a vehicle and a node in infrastructure, it is not possible to classify the communication between a vehicle and a node in road-side that are belonging in same vehicular domain and are accessible with MANET routing, and the communication between a vehicle and a node in the Internet that requires NEMO for mobility support. V2V does not classify the scenario that vehicles exchange the data each other using MANET and the scenario that both vehicles connected to the Internet and exchange the data via the Internet using NEMO.

In order to align with the ITS communication scenario, we rely on the terminology defined in [GeoNet-D.1].

- **Vehicle-based communication modes**
  This mode covers Vehicle-to-Vehicle (V2V) communications without infrastructure support. Communication occurs between a vehicle and another or several vehicles. Applications based on IPv6 as well as other applications not based on IP can be supported, but only IPv6-based communications are in the scope of this study. This mostly concerns safety and traffic efficiency applications

- **Roadside-based communication modes**
  This mode covers Vehicle-to-Roadside, Roadside-to-Vehicle and Vehicle-to-Vehicle communications with infrastructure support. Applications based on IPv6 as well as other applications not based on IP can be supported, but only IPv6-based communications are in the scope of this study. This mostly concerns safety and traffic efficiency applications.

- **Internet-based communication modes**
  This mode covers Vehicle-Internet communications with infrastructure support. Note that any destination reachable through the Internet - including a destination vehicle - is considered as an Internet communication endpoint from the viewpoint of the source. Only applications based on IPv6 are supported. This mostly concerns infotainment, but numerous safety and traffic efficiency applications could benefit from this communication mode.

Chapter 3

Vehicular Communication

Contents

This Chapter provides an overview of all the possible technologies needed in cooperative ITS including network technologies and access technologies. First, physical layer and link layer for wireless technologies are summarized and then, various network protocols are explained. As network layer protocols, a taxonomy is proposed to divide the protocols mainly divided into infrastructure-less class and infrastructure-based class. The infrastructure-less class is known by the research area of MANET. As MANET routing protocols, topological routing and geographical routing are explained. Address auto-configuration mechanisms and in-vehicle Network Discovery are presented as a context of MANET. The infrastructure-based protocols are roughly classified into three categories: Internet mobility support, mobility enhancement and others. Internet mobility support is a set of technologies to allow mobile nodes' application to use a stable IP address as an Identifier while it also allows the packet routing with the other IP address as a Locater in the logical topology. We explain the key technology of the thesis, NEMO and the other mobility support technology. Mobility enhancement is a set of technologies used with the Internet mobility support to supply a better communication to mobile nodes.

3.1 Physical and Link Layer Technologies

Figure 3.1 shows the all the technologies and its categories that described in the Chapter.

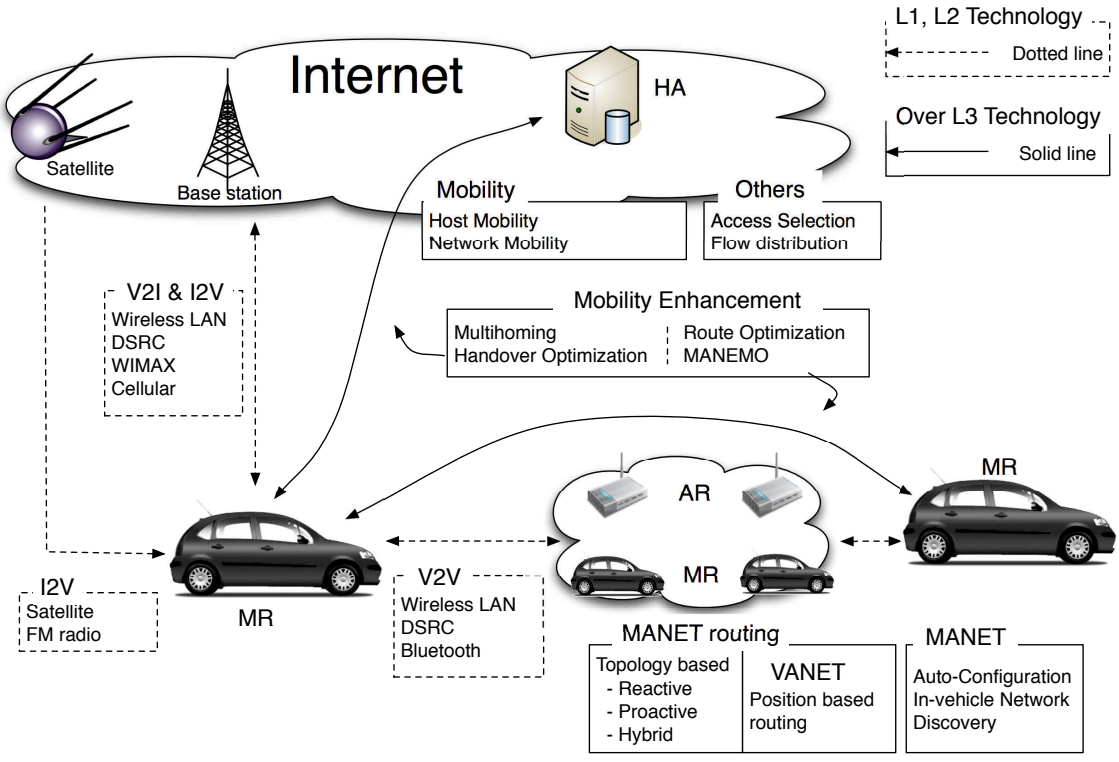


Figure 3.1: State of Arts

It is desirable to select wireless medias to use, because no media cover all over the world and no media are suitable for all the communication for vehicles. The wireless medias are described in the section classified by usage and characteristics and shown in table 3.1. Note that more details in the section are published as [Khaleda2009, Khaled2010].

Generally, wireless medias has two types that are the unicast type with 1-to-1 communication and the broadcast type with 1-to-n communication. The unicast type wireless media is wireless link which connect an access point and a node, or a node to node. In a wireless link, specific sum of bandwidth is determined in specific area, and the nodes connected to the wireless links share the bandwidth. The available bandwidth for a node, thus, decreases when the nodes that connect to the wireless link increase. From this point, there is the tendency that the bandwidth of shorter-range wireless media can be shared by smaller number of nodes, thus greater bandwidth can be available for each node. In contrary, wider-range wireless media has smaller available bandwidth for each node. On the other hand, shorter-range wireless media has less communication stability because of out range of accessible area to access point or frequent access point changes by movement.

Technologies	Range	Data rate	Frequency Band	Standard	Communication		
					V2V	V2I	I2V
Bluetooth	100 m	1 Mbps	2.4 GHz	IEEE802.15.1	✓		
WLAN	200 m	10-50 Mbps	2.4,5 GHz	IEEE802.11a/b/g	✓	✓	✓
DSRC	1 Km	50 Mbps	5.9 GHz	IEEE802.p	✓	✓	✓
WIMAX	10 Km	~20 Mbps	2.4,5 GHz	IEEE802.16e		✓	✓
Cellular	10 Km	~10 Mbps	700~2600 MHz	n/a		✓	✓
RDS/TMC	80Km	1187.5 bps	87.5 ~ 108.0 MHz	CENELEC EN 50067 CEN ENV 12313			✓
Satellite	> 10,000 Km	300~500 Kbps	950~1450 MHz	n/a			✓

Table 3.1: Wireless Technologies

Bluetooth is a wireless standard [IEEE802-15-1-bluetooth] specially created for short range communications between devices usually connected by local ports. Thanks to Bluetooth, however, it is possible to create a *Personal Area Network (PAN)* where several devices can be connected. It operates in the 2.4 GHz band and, due to the low power consumption features, allow communications in a typical range of tens of meters.

Wireless Local Area Network (WLAN) were created to cover connectivity requirements usually fulfilled by common Local Area Network (LAN) technologies, like Ethernet. The set of standards which deal with WLAN features are inside the IEEE802.11x group, and consider a set of protocols which allow devices to be connected to a base station, which is in charge of connecting computers to the rest of the wired network. Among these standards, IEEE802.11a/b/g [IEEE802-11a, IEEE802-11b, IEEE802-11g] specifications are the most known. Although the most used operation mode of IEEE802.11 technologies is the infrastructure mode, using a base station, these devices can also be configured to directly communicate with another device, using the ad-hoc mode. This one is preferred to enable VANET. Many V2V works use WLAN technologies to test multitude of applications, such as cooperative collision avoidance using V2V communications between nearby, or multi-hop manner. For this reason, USA, Japan and Europe have allocated a specific band in the 5.8 and 5.9 GHz for vehicular transmissions, using *Dedicated Short Range Communications (DSRC)* [dsrc]. A variation of the IEEE802.11 standards, IEEE802.11p [IEEE802-11p], is being used as background in the DSRC research. This standard covers the requirements for communicating both periodic and critical information, which allows the deployment of a great variety of vehicular services, using both V2V [ElBatt2006] and V2R [Hattori2004] communications.

Cellular networks have been gradually improved in terms not only of availability all around

the world, but also in the quality of service offered. As a result of applying digital communications to cellular networks, the *Global System for Mobile communications (GSM)* technology achieves the purpose of spreading mobile phones among normal population. Its wide adoption in Europe last years has led the expansion of GSM to other potential markets, like the Chinese one. Many people usually identify the GSM technology as the 2nd Generation mobile telecommunications (2G), which substituted the first one, based on analog technologies. *General Packet Radio Service (GPRS)* appeared with the aim of providing higher data rates than the 9.6 Kbps offered by the standard GSM. It is understood as the intermediate step between 2G and 3G; hence, this is the reason why it is called 2.5G. Last years, the expansion of *Code Division Multiple Access (CDMA)* communication technologies has lead to the appearance of the 3G cellular networks. CDMA2000 and *Universal Mobile Telecommunications System (UMTS)*, this one as the evolution of GSM 2G, are two of the most extended 3G technologies. UMTS offers 384/128 Kbps, but the recent *High Speed Packet Access (HSPA)* improvements offer maximum data rates of 14.4/11.5 Mbps.

Worldwide Interoperability for Microwave Access (WIMAX) is a communication technology which try to fill the gap between 3G and WLAN standards, and it is the first implementation which appears to comply with the *Metropolitan Area Network (MAN)* concept, in a wireless manner. Two main standards are currently considered: IEEE802.16d and IEEE802.16e [IEEE802-16-2009]. The first one is used at fixed locations, and it is a perfect solution for connecting different buildings of a company at a low cost, for example. This specification offers up to 48 Km of coverage and data rates of 70 Mbps. The IEEE802.16e standard [IEEE802-16e], specifically designed for mobile users connected to a base station. IEEE802.16e is, hence, the most appropriate specification of WIMAX for the vehicular field. Tens of Mbps, mobility speed up to 100 Km/h, and 10 km of coverage to the base station, make IEEE802.16e a good option for urban scenarios, where vehicles can be connected at a high data rate using a WIMAX deployment.

The *Radio Data System (RDS)* was developed to carry digital data using the common FM radio band. This allows to multiplex additional information with the audio emission, such as the name of the radio station or the current song, but also it can include a data flag which indicates the receiver it has to pay attention to the broadcasting information because it is being transmitted a traffic bulletin. RDS offers a data rate of 1187.5 bps, and the transmission range offered by FM can reach locations at 80 kilometers far way. The RDS version deployed in U.S. is called *Radio Broadcast Data System (RBDS)* and operates almost identically as RDS , however its usage is less common.

Satellite communication consists of three main entities: sender station, satellite system, and receiver devices. First of all, data is sent from the sender station to the satellite, which is in charge of forwarding the information to receiver devices. Satellite communications offer a very wide coverage and a great broadcast capabilities. It is suited to provide connectivity at remote places, such as mountain areas or islands, but also in developing countries. The data can be sent from an only sender to multiple receivers at the same time and using the same frequency. Thus, satellite communications are suitable for multimedia broadcasting, such as live video, movies and music.

Although sender stations and receiver devices are usually installed at fixed locations, the later ones can be mobile and equipped in vehicles. This kind of architecture is feasible for a unidirectional system providing an Infrastructure-to-Vehicle (I2V) service, however it must be taken into account the important delay which suffer data packets, due to the propagation distance to and from the satellites. The bandwidth obtained in a mobile device is between 300 and 500 kbps. A sender station is usually too big to be brought inside a vehicle, and it requires

a precise orientation to the satellite used. The *Unidirectional Link Routing (UDLR)* [rfc3077] has been standardized to emulate bidirectional communications with a satellite unidirectional link, where mobile terminals receive data using the satellite channel and transmit using other access technologies.

3.2 Taxonomy for Network Layer protocols

The rest of the Chapter of State of the art, we describe the network layer protocols that related to the vehicle communication. Figure 3.2 gives the taxonomy for the network layer protocols that appear in the following sections based on the research areas and target scenarios. The two major categories are classified by the target scenarios that are infrastructure-less scenario and infrastructure-based scenario.

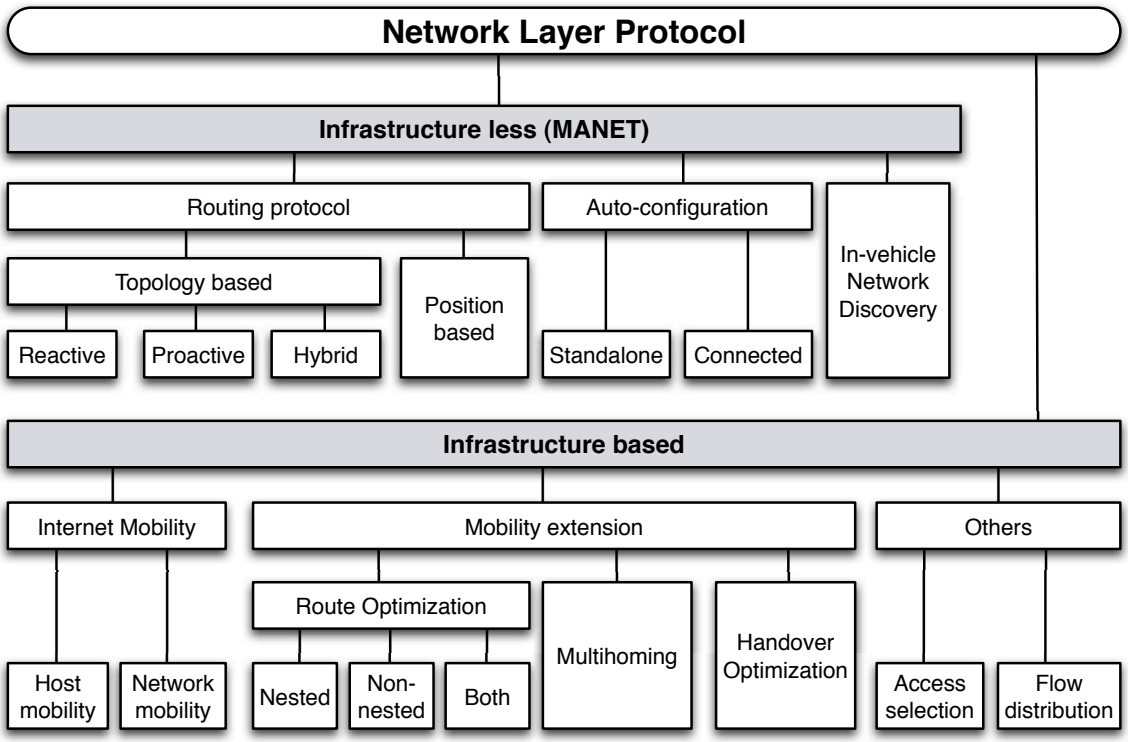


Figure 3.2: Taxonomy

The infrastructure-less scenario is known by the research area of Mobile Ad-hoc Network (MANET). The two main fields that related to the study are routing protocols that concern how the data traffic is routed from the source to the destination in the MANET, and address auto-configuration that concerns how to assign and configure the address in the MANET. The routing protocols are classified into the two classes that are topology-based routing protocol and the position-based routing protocol. Topology-based protocol are divided into three mechanisms by MANET working group in IETF such as reactive, proactive and hybrid. The MANET routing protocols are roughly classified into topology based and position based here, [Murthy2004] provides more category for them. In [Murthy2004], the authors introduce more detailed comparative analysis and taxonomy for MANET routing protocols based on criteria that includes *routing information update mechanism*, *use of tem-*

poral information for routing, *routing topology* and *utilization of specific resources*. On the other hand, there are a lot of proposal in address auto-configuration in MANET. The types of propositions are classified in [draft-bernardos-autoconf-evaluation-considerations] and summarized in [draft-bernardos-manet-autoconf-survey].

The infrastructure-based scenario is roughly classified into the three categories such as Internet mobility support, mobility extension and others. There are many propositions about the Internet mobility support as described in [rfc6301]. In [rfc6301], the authors classifies nearly twenty proposals for Internet mobility support by the criteria based on "*Routing-based Approach v.s. Mapping-based Approach*", "*Mobility-aware Entities*", "*Operator-Controlled Approach v.s. User-controlled*", and "*Local and Global Scale Mobility*". The important classification for vehicular network is whether it is network mobility support. Thus we use simple classification such as host mobility or network mobility.

The mobility extension protocols are the protocols that are based on the Internet mobility protocols and improve the performance as an extension of Internet mobility. The category has three main research fields such as route optimization, multihoming, and handover optimization. The scenarios of route optimization has nested case, non-nested case and both case, and the issues of route optimization of NEMO are addressed in [rfc4888] and the solution space is analyzed in [rfc4889] in IETF. Multihoming is the state that a vehicle maintains multiple network interfaces simultaneously up and has multiple paths to the Internet, that benefits performance and stability of the communication. The possible multihoming configurations offered by NEMO are classified in [rfc4980]. Handover optimization is the category of research that minimizes the impact of disconnection time when the point of attachment to the Internet changes because of movement of mobile nodes. The other protocols that related to the study are the protocols that can be used in the general environment but it can be applied also in mobile environment like the vehicular network.

3.3 Mobile Adhoc Network Technologies

3.3.1 MANET routing protocols

Mobile Ad-hoc Network (MANET) is designed to enable wireless communications in dynamic topologies without any infrastructure. In order to adapt to topology changes, MANET nodes exchange control messages to establish the routes used to forward data packets. MANET has the additional advantage of extending the one-hop communication range, since the packets can be delivered through multiple nodes. MANET routing protocols can be classified into the ***proactive*** ones, where nodes periodically exchange messages to create routes, and the ***reactive*** protocols, in which control messages are exchanged on demand when it is necessary to reach a terminal.

Generally, proactive protocols have the advantage of starting communication rapidly by making the routing table ahead, however, this makes battery life shorter due to frequent signaling. If the topology is highly dynamic and the data traffic is frequent, a proactive protocol could be better. Reactive protocols, on the contrary, keep the battery life longer by reducing signaling messages when there is no data to transmit. The ***hybrid*** protocols that take the advantage of both proactive protocol and reactive protocol by maintaining routes to the near neighbors regularly and searching the destination in long distance on demand.

The examples of protocols in three categories are summarized in Table 3.2. Some routing protocols are specified by IETF MANET working group[manetwg]. Both IPv4 and IPv6 is supported. The *Optimized Link State Routing (OLSR)* [rfc3626] and the *Topology Dis-*

semination Based on Reverse-Path Forwarding (TBRPF) [rfc3684] are specified as proactive routing protocol. And The *Ad hoc On-Demand Distance Vector Routing (AODV)* [rfc3561], the *Dynamic Source Routing Protocol (DSR)* [rfc4728] and the *Dynamic* MANET *On-demand Routing (DYMO)* [dymo] are specified as reactive routing protocol. IETF standardizes proactive and reactive protocols, however not hybrid protocols.

As non-standardized proactive MANET routing protocols, *Wireless Routing Protocol (WRP)* [WRP], *Clusterhead Gateway Switch Routing protocol (CGSR)* [CGSR] and *Destination-Sequenced Distance-Vector routing (DSDV)* [DSDV] are proposed. And *Temporally-Ordered Routing Algorithm (TORA)* [TORA] and *Associativity-Based Routing (ABR)* [ABR] are proposed as non-standardized reactive MANET routing protocols. *Zone Routing Protocol (ZRP)* [ZRP], *Core Extraction Distributed Ad hoc Routing (CEDAR)* [CEDAR] and *Zone-based Hierarchical Link State Routing Protocol (ZHLS)* [ZHLS] is proposed as the hybrid protocols. Multi path MANET solutions are proposed and they can be seen in survey paper[multipath-manet].

	Standard in IETF	Non Standard in IETF
Proactive	OLSR[rfc3626], TBRPF [rfc3684]	WRP [WRP], CGSR[CGSR], DSDV [DSDV]
Reactive	AODV[rfc3561], DSR [rfc4728], DYMO[dymo]	TORA [TORA], ABR [ABR]
Hybrid	—	ZRP [ZRP], ZHLS [ZHLS], CEDAR [CEDAR]

Table 3.2: MANET classification

3.3.2 Geographic routing and GeoNetworking

3.3.2.1 Various Geographic routings

Vehicular Ad-hoc Network (VANET) are a particular case of MANET, which are characterized by battery constraints free, high speed, GPS-equipped nodes, and regular distribution and movement. First, vehicles have a larger battery than mobile terminals or sensor devices, which is also charged when the engine is running. Second, the speed of vehicles is also higher than common portable terminals, and relative speeds can reach 300 Km/h; hence the duration of the routing entries is extremely short. Third, a GPS device can be assumed in many cases, whose information improves the network performance in some proposals. There is currently a debate among the pioneer about redefining the acronym VANET to de-emphasize ad hoc networking. Because the discussion has not yet reached consensus, the term can be referred as vehicle-to-vehicle and vehicle to roadside communication [Hartenstein2008].

Unlike topology based routing, geographic routing does not need to maintain the routing table to know the topology. Thus geographic routing can eliminate the problem of topology based routing that found route becomes quickly unavailable when topology change is very frequent because of topology change propagation delay. In geographic routing forwarding, the intermediate nodes make a decision based on the destination position and neighbor positions. Because of this fact, geographic routing shows strength for highly dynamic environment like vehicular network.

A survey on position-based routing in mobile ad hoc networks is provided in [Mauve2001]. *Location-Based Multicast (LBM)*[Ko1999], *Greedy Perimeter Stateless Routing (GPSR)* [Karp2000]

and *GVGrid* [Sun2006, Sun2006a], improve routing tasks by using Global Positioning System (GPS) information, for example. Finally, the movement and density of the nodes are not random, since vehicles drive on roads, that makes the nodes position somehow predictive. This concept can be used to detect stable structures or clusters to improve the network performance. Some other protocols try to send packets only to a set of nodes located in a geographical zone (*geocast*), such as *GeoGRID* [Maihfer04, liao00], for example. Here, the geographic area is divided in 2D logical grids. In each grid, one node is elected as the gateway, and only this one is allowed to forward messages.

3.3.2.2 GeoNetworking

Since geographic routing is suitable for vehicular network, standard for geographic routing is strongly demanded. As explained in Section 2.2, the ITS Station (ITS-S) architecture has geographic routing protocol as network layer protocol. It is also in the report [COMeSafety-final] of consolidation process in Europe by COMeSafety. ETSI addresses the requirements for geographic routing for vehicular communications in [ETSI-TS-102-636-1-req]. Then it summarizes all the possible scenarios for GeoNetworking in [ETSI-TS-102-636-2-Scenario]. The specification of geographic routing is being standardized in [ETSI-TS-102-636-4-1-Media, ETSI-TS-102-636-4-2-Media]. In addition to the standardization, C2C-CC makes a specification of C2CNet based on the architecture described in Section 2.1.3. IPv6 over C2CNet of GeoNet project is detailed in Section 2.1.2.1. As unicast forwarding mechanism, the GPSR protocol is adopted in GeoNet project [GeoNet-D.2].

The C2CNet is one of geographic routing (see Section 3.3.2.1 for details) that is specified in C2C-CC. This protocol would define a separate C2CNet header with a separate C2CNet identifier, tentatively 64-bit length, identifying C2CNet node.

Four types of communication are defined in GeoNet project: *GeoUnicast*, *GeoBroadcast*, *GeoAnycast* and *TopoBroadcast* [GeoNet-D.2]. First three are the type of communication which based on geographic information and the last one is based on network topology information. *GeoUnicast* routes data from a source node to a destination node for which the exact geographical location is known. As *GeoUnicast* routing, the GPSR[Karp2000] is adapted. *GeoBroadcast* delivers data from a source node to all nodes located within a specific geographical area. And *GeoAnycast* routes data from a source node to any node located within a specific geographical area. *TopoBroadcast* routes data from a source node to all nodes located up to a specific distance in terms of hops.

GPSR is a position based routing protocol. The header of the data has the destination's position (latitude, longitude and altitude). And the nodes maintain the neighbors' position information in location table instead of topology information in the routing table. The GPSR has two modes as shown in figure 3.3 such as greedy forwarding mode and perimeter forwarding mode.

In the Greedy forwarding, the sender selects the closest forwarder to the destination node. The packets are sent to obtain the maximum gain to the destination and they are progressively forwarded to the destination. The greedy forwarding mode is taken when there is closer next hop neighbor to the destination. In the left of figure 3.3, the source node choose node '3' that is the closest neighbor to the destination.

On the other hand, when no other node can obtain the gain to the destination, the perimeter mode is taken. The mode is necessary when there are no closer neighbor to the destination because of obstacle or no road. In this mode, the packet is forwarded closer faces of a planar sub-graph of the full radio network connectivity graph, until reaching a node

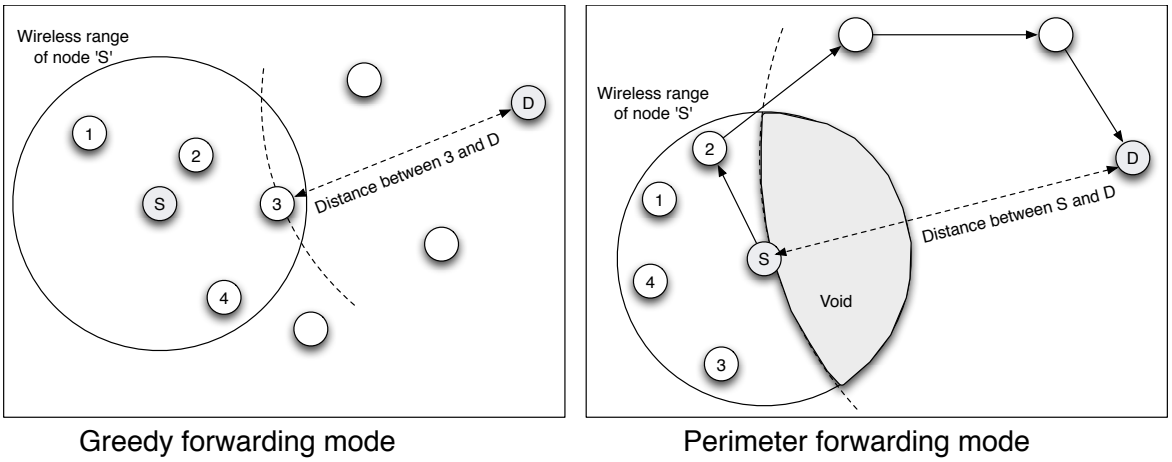


Figure 3.3: Greedy Perimeter Stateless Routing (GPSR)

closer to the destination.

In the right of figure 3.3, there is no node in the area of 'void', and this means no neighbor nodes of the source node make positive progress to the destination. The source node seeks the route around the region of 'void' to forward the packet beyond the region of 'void'. And the source node selects the node '2' as a next hop.

In above example, each node knows the position information of the neighbor nodes thanks to beaconing that periodically sent from each node. The beacons reaches only to the neighbor nodes since the message is broadcasted in single hop scope. The beacon includes C2CNet ID, latitude, longitude, altitude, speed, heading and time stamp. Exchanged information is stored in the location table in each node. Table 3.3 is the content of the packet and data structure of C2CNet used in the GeoNet project [GeoNet-D.2]. These items are also included in C2C-CC specification.

Item	Format	Description
C2CNet ID	64 bit address	The identifier of the C2CNet interface
Latitude	32 bit signed integer	WGS-84 latitude expressed in 1/10 micro degree
Longitude	32 bit signed integer	WGS-84 longitude expressed in 1/10 micro degree
Altitude	16 bit signed integer	Altitude of the vehicle expressed in signed units of 1 meter
Speed	16 bit signed integer	Speed of the vehicle expressed in signed units of 0.01 meter per second
Heading	16 bit unsigned integer	Heading of the vehicle expressed in unsigned units of 0.1 degrees from North
Time Stamp	16 bit unsigned integer	The time stamp that the geographic position is recorded in UTC.

Table 3.3: Parameters of Location Table

C2CNet can deliver the packet to the destination with geographic position. However in the case that the communication source does not know the destination position, the source should

resolve the position by C2CNet ID. Location service realizes the resolution of the position of nodes from C2CNet. Location service can be any kinds of position resolution including client-server manner. An example of location service is broadcast based. A C2CNet node sends broadcast message to ask the position of a node and any node that knows the position of the node replies the position.

Obtained geographical position is set in the destination of C2CNet header in the case of GeoUnicast as shown in Figure 3.4. Source node position vector includes, C2CNet ID, latitude, longitude, altitude, speed, heading and time stamp. On the other hands, Figure 3.5 shows the C2CNet header for GeoBroadcast packet. The destination of GeoBroadcast is indicated by the geographical location of center of destination area and the radius of the circle area.

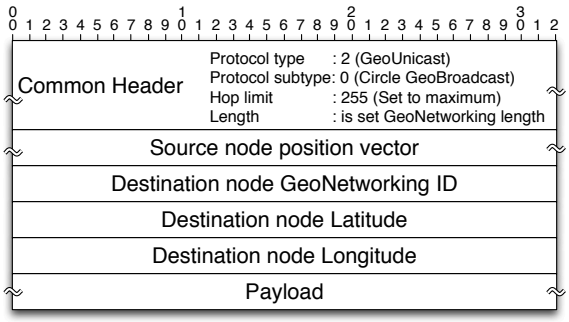


Figure 3.4: GeoUnicast packet

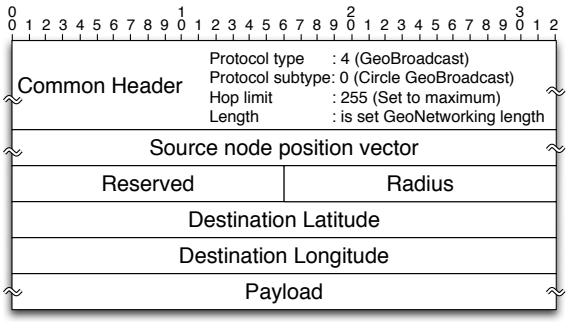


Figure 3.5: GeoBroadcast packet

3.3.3 Auto-configuration in MANET

Address auto-configuration consists of both functionality of address assignment and Duplicated Address Detection (DAD). IPv6 protocol allows a host to configure its own address either in stateful way [rfc3315], stateless way [rfc4862] or static way. Upon generating a tentative IPv6 address, the host should perform DAD as of Auto-configuration [rfc4862] to guarantee the address uniqueness on a link.

In DAD procedure, the node that generates the address sends the Neighbor Solicitation (NS) message to the all-node multicast (broadcast) with tentative address on a link. In the case that the other node already using same address with the tentative address receives the NS message, then replies the Neighbor Advertisement (NA) message. Address uniqueness of the tentative address is guarantied after waiting $DupAddrDetectTransmits \times RetransTimer$. The $DupAddrDetectTransmits$ is defined in [rfc4862], which is the number of consecutive NS messages sent while performing DAD on a tentative address. And the $RetransTimer$ is defined in [rfc4861], which is the time between retransmissions of NS messages to a neighbor when resolving the address or when probing the reachability of a neighbor. Default value of former is determined as 1 and later is determined as 1,000 milliseconds.

Current DAD employs solicitation/advertisement mechanism by assuming the links have broadcast capability. This assumption have made on the Ethernet link when the nodes were connected with wired cable. Today, in vehicular network scenario, the assumption can be broken because of appearance of different links. In MANET link, this makes problems because of absence of DAD scope that caused by link-local scope limitation and nature of high mobility.

First, one-hop neighbors are connected in a physical link. Since current DAD works on link-local scope, there is the possibility that an address is duplicated farther than two hop neighbors. Almost all of MANET routing protocols supports flooding to reach all the nodes in MANET could beyond one-hop neighbor, DAD can be performed with flooding scheme. However there is no clear scope in multi-hop environment. This results that the uniqueness of the address cannot be guaranteed however long distance the packets is transmitted. Second, one-hop neighbors may be changed frequently because of high mobility of nodes. This results that two same unique addresses in different link scopes can be duplicated when they meet each other. Since members of a MANET could be changed frequently, the flooding approach cannot work with the same reason.

IP Auto-configuration for MANET has been investigated in Autoconf working group and MANET working group in IETF. [draft-ietf-autoconf-manetarch] presents the initial motivation for MANET and describes unaccustomed characteristics and challenges. Auto-configuration consist of both of IP address assignment and DAD. A lot of effort already has been made and many proposition have appeared in the research area. The types of propositions are classified in [draft-bernardos-autoconf-evaluation-considerations] and summarized in [draft-bernardos-manet-autoconf-survey]. Since DAD is fundamental functionality to start communication with IP, there are strong demands to investigate it further. In [draft-ietf-autoconf-statement], the two main scenarios are defined, which are standalone MANET scenarios and connected MANET scenarios. The former is the autonomous ad hoc network that is not connected to any external network. And the later is ad hoc networks having connectivity to one or more external networks, typically the Internet, by means of one or more gateways. In vehicular network scenario, we take the target of the connected MANET scenarios. In connected MANET scenarios, some of them focus on address assignment with stateless auto-configuration and DAD is out of focus [draft-wakikawa-manet-globalv6]. There are some approaches integrated on specific MANET routing protocol [draft-ruffino-manet-autoconf-multigw, draft-ros-autoconf-emap, draft-cha-manet-extended-support-globalv6]. Some takes Dynamic Host Configuration Protocol (DHCP) [draft-clausen-manet-address-autoconf] approach because the address uniqueness can be guaranteed by allocating from available address pool in DHCP server. *Vehicular Address Configuration (VAC)* [Fazio2006] adapts DHCP approach to the group of vehicles by one leader taking role of DHCP server. *Multi-hop Radio Access Network (MRAN)* [draft-hofmann-autoconf-mran] targets on multiple Internet gateway and solves problem for handover. Address uniqueness is guaranteed by assuming the identifier of each node is globally unique in the other proposition [draft-laouiti-manet-olsr-address-autoconf].

3.3.4 In-vehicle Network Discovery

MANET routing protocols originally aim for routing from the ID (ex. address) of source MANET node to the ID of destination MANET node. On the other hand, in vehicle network scenarios, the source and the destination are connected behind the MANET node. In other word, MRs participate the MANET cloud and the MNNs connect to the in-vehicle network behind the MRs. To route the packet from source MNN to destination, the in-vehicle network prefix have to be exchanged among the MANET cloud. Moreover, an MR should maintain the other MR ID with its in-vehicle network prefix. The matching between MR ID and the in-vehicle prefix is the key point for in-vehicle network discovery.

Since the in-vehicle network prefix is matching, between IP address and network prefix, there are already several propositions. The most primitive one is static configuration in the routing table. Otherwise there are routing protocols to make a matching between IP ad-

dress and network prefix such as Open Shortest Path First (OSPF) [rfc5340] and Routing Information Protocol (RIPng) [rfc2080]. OLSR [rfc3626] provides Host and Network Association (HNA) to find network behind OLSR nodes which connect to non-OLSR interface. HNA message is typically used for discovering in-vehicle network in the case of vehicular network because in-vehicle nodes may not have OLSR functionality.

[draft-jhlee-mext-mnpp, draft-petrescu-autoconf-ra-based-routing] extends the Router Advertisement (RA) and router Router Solicitation (RS) messages defined in Neighbor Discovery Protocol (NDP) to announce the Mobile Network Prefix (MNP) assigned to a vehicle to other vehicles or the roadside infrastructure on the same wireless link. In proactive mode, extended RA is sent periodically into the MANET cloud. In reactive mode, RS message is sent to solicit the reply to all node multicast in the MANET network. The MR upon reception of the Mobile Network Prefix Provisioning (MNPP) Solicitation messages immediately sends the solicited MNPP Advertisement messages including the MNP being used in its in-vehicle network.

To exchange in-vehicle network prefix, there are some possible security threats such as redirect attack, replay attack, wormholes, tracking and so on. MNPP[draft-jhlee-mext-mnpp, GeoNet-D.2, Lee2011] enhances security to overcome these security issues. Authors claim that the following requirements should be fulfilled in MNPP: Message Authentication and Integrity, Address Ownership, MNP Authorization, Anti-Replay, Anti-Wormhole, Message Non-repudiation and Hiding Identity.

3.4 Mobility Technologies

The IP was standardized with assumption that the nodes do not move frequently without shutting down the application because of their weight, wires, and electric line. Today, thanks to reducing the weight, wireless technologies and battery performance, nodes in the Internet moves around. In such environment, as a node move to other link, the IP address of the node changes. The address change caused by mobile nodes' movement arises mobility issues. The application running on a mobile node needs to use a stable IP address as an *Identifier*, but the topological location does not allow to use the unchanged IP address, because the IP address works as a *Locater* in the logical topology in the packet routing. Mobility technology is mapping between the Identifier and the Locator. The section introduces Mobile IPv6, NEMO, Multiple Care-of Address registration and other protocols.

3.4.1 Mobile IPv6

Mobile IPv6 is the host mobility support protocol standardized as [rfc6275] in IETF. The protocol allows a *Mobile Node (MN)* to change the point of attachment one link to another with uninterrupted Internet connectivity. MN can connect to the Internet with a permanent and unchanged address named *Home Address (HoA)*. A node communicating with MN is called *CN* and packets destined from CN to HoA are delivered to the *home link* of the MN by normal Internet routing. A fixed router called Home Agent (HA) captures the packets and forward them to the current point of attachment of MN by IP-in-IP tunnel. An MN configures an address called *Care-of Address (CoA)* in *foreign link* and always notifies the address to the HA. The HoA, the CoA and lifetime are included in the notification message called *Binding Update (BU)*. The HA receives the BU and replies *Binding Acknowledgement (BA)* to notifies the acceptance of the BU to the MN. An HA has conceptual data base called *Binding Cache (BC)* to maintain the binding between HoA and CoA. The entries of BC are

updated by BU and BA signaling, or expire by the lifetime. MN, on the other hand, maintains *Binding Update List (BUL)* to store the address of the nodes that maintain BC. The signaling messages between nodes and Binding database are illustrated in Figure 3.6. When MN does not have any HA address, MN sends Dynamic Home Agent Address Discovery (DHAAD) request to anycast address in the home link in order to get the HA address list in DHAAD reply from an HA.

In Mobile IPv6, all the packet between a CN and an MN goes through the HA that supports MN's mobility. To avoid suboptimal route, [rfc6275] define a Route Optimization (RO) mechanism to solve the problem. The solution to establish direct path between CN and MN with mobility is illustrated in Figure 3.6. After the communication starts between MN and CN, the MN can try to move the BC from the HA to the CN. The MN sends BU to the CN after Return Routability procedure. The procedure guarantees that the binding between the HoA and CoA is correct (The both address are routed to the MN). This is verified by sending test signaling message from both of HoA and CoA (thus via HA and direct to CN). *Home Test Init (HoTI)* and *Home Test (HoT)* are the request and reply message via the HA respectively, and *Care-of Test Init (CoTI)* and *Care-of Test (CoT)* as well respectively. Once return routability successes, CN maintain BC and the MN store CN address in the BUL. The MN sends BU to both the HA and the CN.

In Internet Research Task Force (IRTF) IP Mobility Optimizations (Mob Opts) Research Group (RG), researchers discuss the enhancement of Mobile IPv6 RO to perform it with low latency, strong security, reduced signaling, or increased robustness [rfc4651]. Enhanced RO for Mobile IPv6 [rfc4866] is specified as an amendment to route optimization in base Mobile IPv6 [rfc6275]. It secures a mobile node's home address against impersonation using *Cryptographically Generated Addresses (CGA)* [rfc3972] based home address. It also eliminates the latency of the HoA and CoA tests are in most cases, allowing mobile and correspondent nodes to resume bidirectional communications in parallel with pursuing a CoA test. Cryptographically generated home addresses and concurrent CoA tests are preferably applied together, but a mobile node may choose to use only one of these enhancements.

3.4.2 NEMO

The NEMO Basic Support [rfc3963] is the network mobility support protocol specified at IETF, while Mobile IPv6 is host mobility. NEMO is designed based on Mobile IPv6. To support network mobility, a router called MR manages mobility in behalf of all the nodes in mobile network. Thus the nodes inside the mobile network named MNNs are standard IPv6 nodes without mobility management functionalities. The MR sends a BU to the HA like as Mobile IPv6, but in NEMO, the *MNP* are included in the message. This prefix is stored in the HA as the NEMO prefix table with the BC. The packets from CN that are destined to the MNP are captured at the HA and forwarded to the MR with the IP-in-IP tunnel. The MR decapsulates the tunnel and sends it to the MNN. The signaling messages between the nodes and Binding database are illustrated in Figure 3.6. The goals of NEMO and the related terminology are described in [rfc4886] and [rfc4885], respectively.

3.4.3 Multiple Care-of Address Registration

Mobile IPv6 and NEMO basic support configure a tunnel between HA address and CoA of MN and MR respectively, even if MN and MR has several network interfaces. This is because an HoA correspond a CoA in these mobility technologies. Multiple Care-of Addresses Registration (MCoA) [rfc5648] is thus proposed as an extension of both Mobile IPv6 and

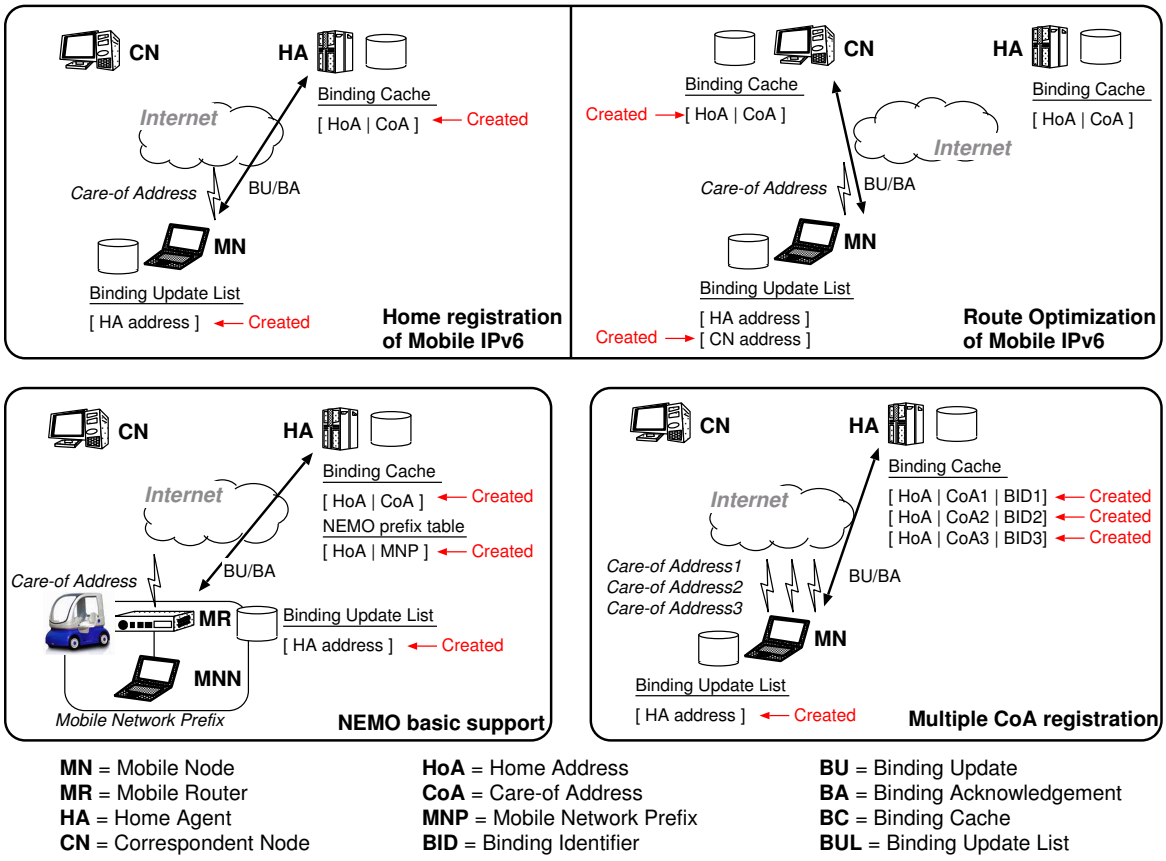


Figure 3.6: Binding Management of Mobility technologies

NEMO Basic Support to establish multiple tunnels between MR and HA. Each tunnel is distinguished by its *Binding Identification number (BID)*. The multiple CoAs are registered with BID in the BC at HA and CN as in Figure 3.6. In other words, Mobile IPv6 and NEMO Basic Support only realizes interface switching while MCoA supports simultaneous use of multiple interfaces. An MN and an MR can register multiple CoAs at once by sending a single BU to the HA, that defined as bulk registration. This is useful to save the number of the signaling messages between the nodes.

3.4.4 Other Mobility Protocols

Mobility protocols diverge by approaches how to map between a stable and unchanged node Identifier and Locator representing the node's current location. [rfc6301] introduces nearly twenty mobility protocols proposed in literature. The mobile technologies are classified in table 3.4. The number in parentheses is the year that the protocols were first proposed. There are three main axes to classify the approach of mobility protocols: 1) Routing-based v.s. Mapping-based, 2) Global v.s. Local scale and 3) mobility aware entity.

Concerning about update route to the mobile node, there are mainly two approaches that is routing based approach and mapping based approach. Routing based approach updates mobile node's current location using dynamic routing protocol. Two sub-classes are divided by the way of propagation of mobile nodes' location information. Broadcast based sub-class broadcast the location information in the network, in contrary, a host-based path is

maintained by the routing system. In mapping based approach, mobile node's location is maintained by the anchor that is in charge of mobility support instead of notifying the location to all CNs in the Internet all the time. *Wide-Area IP Network Mobility (WINMO)*[Hu2008] takes hybrid approach of routing based and mapping based to obtain the benefits of both approaches (It is omitted in table 3.4).

The Second axis is whether it is global or local scale mobility. Global mobility works no limitation of mobile node's moving area. It focuses more scalability of the protocol. On the other hand, the local scale mobility protocols focus more the efficiency of the protocols and performance of mobile nodes' communication such as handoff delay and handoff loss. Local scale mobility protocols usually work together with global mobility and contribute the improvement of performance of mobile nodes' communication.

	Mapping-based			Routing-based	
	Mobile node based	Network based	End node based	Broadcast	Path
Global	VIP (1991) [Teraoka1991], LSR (1993) [LSR], Mobile IP (1996) [rfc6275], LIN6(2000) [LIN6], NEMO (2000) [rfc3963], DSMIPv6 (2005) [rfc5555], Global HAHA (2006) [?]		E2E (2000)[E2E], M-SCTP (2002)[M-SCTP], HIP (2003)[rfc5201], ILNPv6 (2005)[ILNPv6], BTMM (2007) [rfc6281], LISP-Mobility (2009) [draft-meyer-lisp-mn]	Connexion (2004) [Dul2006]	MSM-IP (1997)[MSM-IP]
Local	HMIP (1998)[rfc5380], FMIP (1998) [rfc5568]	PMIP (2006) [rfc5213]		Columbia (1991) [Columbia]	Cellular IP (1998) [CellularIP], HAWAII (1999) [HAWAII], TIMIP (2001)[TIMIP]

Table 3.4: Mobility Protocols

The third point is about mobility aware entity in mapping based approach. There are four related entities for mobility support that are MN, CN and anchor that maintains the mapping between MN's identifier and locator, and network. The protocol design depends on which entities involves to mobility support and they hides movement of MN from which entities. Depending on combination of mobility aware entities, the mapping based mobility protocols are classified into three approaches as shown in Figure 3.7 such as:

- Mobile Node based,
- Network based, and
- End nodes based

Mobile Node based approach is designed to hide the MN's movement from CN by MN and anchor supporting mobility. The network is kept untouched. The identifier and the locator are mapped in the anchor, and the CN keeps using the unchanged IP address (identifier) as a destination address thanks to the translation from the identifier to the locator in the anchor.

The Network based approach takes the design to hide the movement from both MN and CN by the anchor and the network that MN is attached supporting mobility. Basically the MN does not notice the movement when access point changes because the network announce always same network prefix.

In End nodes based approach, MN and CN is mobility aware nodes. The mapping between Identifier and locator of MN are maintained in both ends. As a result, the anchor that maintains the mapping is not necessary. In the approaches, dynamic Domain Name System (DNS) is commonly used to track the MN's current location. MN updates DNS entry as it moves to the new access network to keep the new location in the server.

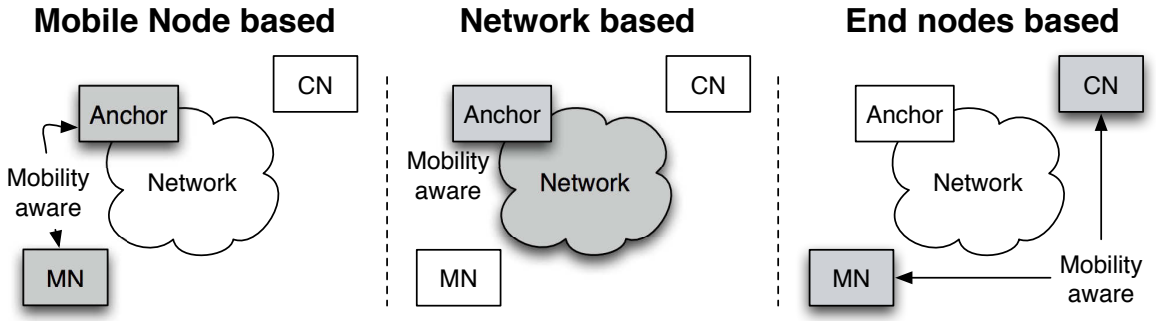


Figure 3.7: Mobility aware entity classification

3.5 Mobility Enhancement Technologies

3.5.1 Multihoming

MRs can ship multiple network interfaces such as IEEE802.11a/b/g, WIMAX, GPRS/UMTS, that have different characteristics as shown in section 3.1. When an MR maintains these interfaces simultaneously up and has multiple paths to the Internet, it is said to be multihomed. In mobile environments, MRs often suffer from scarce bandwidth, frequent link failures and limited coverage. Multihoming brings the benefits of alleviating these issues [draft-ietf-monami6-multihoming-motivation-scenario, draft-ietf-monami6-mipv6-analysis]. Simultaneous usage of all the connection is motivated by the users and applications for more network performance (Ubiquitous access, redundancy, fault recovery, load balancing, load sharing, bi-casting, preference setting, increased bandwidth, decreased delay).

The possible configurations offered by NEMO are classified in [rfc4980], according to three parameters: (x) the number of MRs in the mobile network, (y) the number of HAs serving the mobile network, and (z) the number of MNPs advertised in the mobile network. NEMO basic support has "single MR, single HA and single MNP" configuration, referred to as $(x, y, z) = (1, 1, 1)$. In this configuration, a tunnel is established between the HA address and a CoA of the MR in NEMO Basic Support, even if the MR is equipped with several interfaces. With MCoA [rfc5648] support explained in Section 3.4.3, MR and HA can maintain multiple paths between them in the configuration of $(x, y, z) = (1, 1, 1)$. [? Ronan2008] apply Site Multihoming by IPv6 Intermediation (SHIM6) [rfc5533] to the mobility protocols to make the mobile node multihomed in the configuration.

Concerning about multiple mobile routes ($(x, y, z) = (n, *, *)$), [mr-cooperation-analysis] provides the scenarios, analysis and possible solutions. A mobile router acts as a gate-

way in in-vehicle network, and in addition to the router, the passenger brings the mobile devices as mobile routers. Multihoming is realized by sharing the connectivity to the Internet among these mobile routers. Or multiple MRs are fixed in vehicle in order to increase the robustness, or to apply different security policy to in-vehicle networks [Tsukada2005, Paik2004, Paik2008b, Paik2004a, Ng2004, Kuntz2008a].

3.5.2 Access Selection

When multiple paths to connect to the Internet via several wireless network interfaces shipped on MR, there is the demand to select the best interface in order to provide the most satisfaction of application users. An "Always Best Connected (ABC)" scenario, where a person is allowed to choose the best available access networks and devices at any point in time, is presented in [Flstad2009, Gustafsson2003].

The decision for access selection depends on various application demands and multiple criteria. Application demands are for examples as follows: cost, power consumption, bandwidth, loss rate, connection stability, security, jitter, possibility of availability. [Alshaer2009, BenRayana2009] propose to introduce intelligent route selection by applying certain policy to the flows in an MR.

[RAYANA2010] assumes three different parties (Mobility Framework Administrator, 3rd party operator and user application) that are related to the interface selection as shown in Figure 3.8. The Mobility Framework Administrator configures the high-level policy of the MR and HA and 3rd party operators configures the policy of access network as well as Internet Service Provider (ISP). Interface selection decision takes into account these high-level policies coming from the administrator and also from operators as shown in Policy Management in Figure 3.8. The high-level policies are stored in Flow database and Network Database.

User applications in the MNNs send the flows to the MR and the MR has monitoring function of flow as well as the monitoring of access networks. In decision process, the satisfaction scores are calculated based on the estimation in the case that a certain flow goes through a certain access network. The metrics of the score calculation are called Objective such as, for example, cost, power consumption, bandwidth, loss rate and so on, as shown in Figure 3.8.

The Mobile Framework Administrator gives weights to each objective in order to specify putting importance on which objectives (grey cells). Minimum requirement of the flows for both upload and download traffic is given to the second column (blue cells). Then all the possible access network performances are filled in the last columns per both upload and download of each network interfaces based on monitoring and database (orange cells). The operator policy is taken into account based on the recommendation of the access network in form of weight such as mandatory, optional, not mentioned, unadvised and forbidden (Green). These scores are calculated for all the flows and the mode of the flows (Cost Economy, Energy Savings, Better Performance). [BenRayana2009, RAYANA2010] proposes using the *Ant Colony Optimization (ACO)* algorithm in order to obtain acceptable solutions in a polynomial time. Flow filtering rule that is detailed in section 3.5.4 is set by the Flow routing module according to the best solution and fast recovery solution. The Interface Management is responsible for the activation/deactivation of the interfaces in order to save battery as told by the decision algorithm's best solution. The Application Adaptation module sends feedback to the mobility-aware application running on an MNN. About feedback, the authors propose following two models: Centralized Decision Communication Model, Distributed Decision Communication Model. In former model, the MR provides a specific answer to each

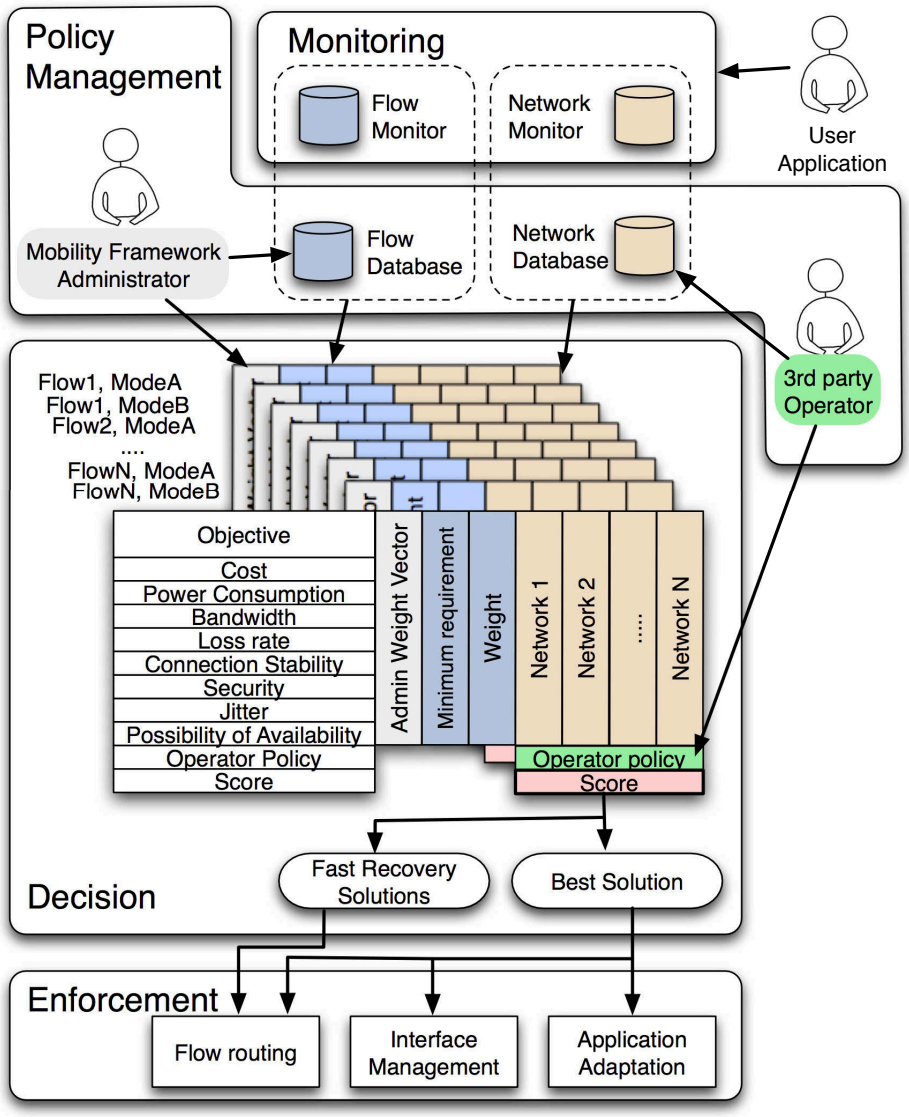


Figure 3.8: A Smart Management Framework for Multihomed Mobile Router

application in order to realize fairness between applications. On the other hand, in the later model, MR broadcasts the available resource level in the mobile network and each application takes a decision.

Wiffler proposed in [Balasubramanian2010] leverages the presence of Wi-Fi networks to offload 3G cellular traffic, for example, for smartphone in vehicle. The system does not use standardized mobility support such as Mobile IP, but use a *Wiffler* proxy router as an anchor point. The decision of switching 3G and Wi-fi is taken with the two key ideas (*leveraging delay tolerance* and *fast switching*) to avoid the packet loss in Wi-fi in moving environment. *Wiffler* tries to send delay tolerant application data to Wi-fi network by using delay tolerance metrics defined to each application, because a user may be willing to tolerate a few seconds delay to send their email or complete a file transfer if it reduces 3G usage. *Wiffler* uses also link-layer information to enable fast switching to 3G in the face of poor WiFi conditions. The algorithm is quite simple that a mobile node sends the packet on 3G if the WiFi link-layer

fails to deliver the packet within a delay threshold. There are two motivations behind of the algorithm, that are because 1) that waiting for WiFi link-layer retransmissions incurs delays and 2) there is a high chance that the retransmission will fail, since losses are bursty in the vehicular environment [Balasubramanian2008, Srinivasan2008].

3.5.3 Handover Optimization

The process of switching one network to another is called handover. It is divided into three types of scenario which are L2 horizontal handover, L3 horizontal handover and vertical handover. Horizontal handover refers to the handover between same media. L2 horizontal handover is switching between access points that have same subnet and same media. On the other hand, L3 horizontal handover is switching between access points that have different subnet and same media. Vertical handover is the handover between different medias and different subnet.

In mobile environment, re-registration of location is necessary for L3 handover. In Mobile IPv6 and NEMO case, the registration means sending binding update and receiving binding acknowledgement on the mobile node. During the re-registration period, some packets are lost. Thus some handover optimizations are proposed.

Fast Handovers for Mobile IPv6 (FMIPv6)[rfc5568] optimizes the handover latency by reducing the movement detection latency and the new CoA configuration latency. The mobile nodes find next AR in advance before handover by extended AR functionality. FMIPv6 defines proactive fast handover and reactive fast handover that are correspondent to make-before-break and make-after-break handover, respectively.

Hierarchical Mobile IPv6 (HMIPv6)[rfc5380] is designed to reduce the amount of mobility signaling by Mobility Anchor Point (MAP) that is proposed in the document. A MN in a MAP domain receives RAs with one or more MAPs information. The MN registers the CoA to the MAP that acts like as HA. The actual HA has the MAP address as a CoA. In local MAP domain, the MN only needs to register the CoA to the MAP not to HA, thus the movement is hidden from the actual HA. The binding signaling between a MN and MAP has less latency because there are nearer than between the MN and HA.

A MN decides the handover based on network layer information such as NDP or RA. However link layer information is also important to optimize the handover. Such a information includes link-up, link-down, radio signaling strength and etc. Handover Optimization and L2 Abstractions [rfc5184] defines nine kinds of L2 abstractions in the form of "primitives" to achieve fast handovers in the network layer. This mechanism is called "L2−driven fast handovers" because the network layer initiates L2 and L3 handovers by using the primitives.

3.5.4 Flow Distribution

To transfer data into multiple interfaces, policy based flow distribution is proposed. The traffic can be distributed into multiple paths by source and destination address, source and destination port, flow type and so on. In NEMO basic support, traffic comes from the Internet to the mobile network is distributed in the HA, and the opposite way of traffic is distributed in the MR. So the neither MR or HA is not able to change round-trip paths, when it changes the policy database. In this case, the incoming and outgoing paths can be asymmetric, and it may not satisfy the user's demand. Thus, policy synchronization between the MR and the HA is needed. Some proposals have appeared in IETF. [rfc6088, rfc6089] propose to extend binding update and binding acknowledgement messages to bind flows to the Binding Identification number (BID). Flow binding

option are introduced for the purpose. This is implemented in Linux[1] in [Ropitault2008]. [draft-larsson-mext-flow-distribution-rules, Mitsuya2007] specifies an OS independent rule language to describe to allocate the flows to the paths in multihomed nodes. The generalized the flow distribution language is proposed for important multihoming technologies (MCoA support for MIPv6/NEMO, Host Identity Protocol (HIP)[rfc5201], SHIM6 [rfc5533] and Stream Control Transmission Protocol (SCTP) [rfc4960]). The transfer of the rule set to the communicating peers is outside the scope of [draft-larsson-mext-flow-distribution-rules, Mitsuya2007] and the method is proposed in [draft-eriksson-mext-mipv6-routing-rules]. The routing rules signaling is transmitted in Generic Notification Messages (GNM) proposed in [draft-haley-mext-generic-notification-message].

3.5.5 Route Optimization in NEMO

NEMO is one of key technologies of vehicle communication, however, the issues related to Route Optimization still remain in NEMO Basic Support, while they already have been solved in Mobile IPv6 [rfc6275]. In NEMO, all the packets to and from MNNs must be encapsulated with IP in the tunnel between the MR and the HA. Thus all these packets between MNNs and CNs must go through the HA. This causes various problems and performance degradation. These sub-optimal effects are described as follows.

Suboptimal routes are caused by the packets being forced to pass by the HA. This leads to increased delay that is undesirable for applications such as real-time multimedia streaming. **Packet Encapsulation** of additional 40 bytes header increases packets overhead and risks of packet fragmentation. This results in an increased processing delay for every packets being encapsulated and decapsulated in both the MR and the HA. **Bottlenecks in the HA** are a severe issue because significant traffic to and from MNNs is aggregated in the HA when it supports several MRs acting as gateways for several MNNs. This may cause congestion at the HA that would lead to additional packet delays, or even packet losses. **Nested Mobile Networks** is an issue that NEMO Basic Support raises by having arbitrary levels of nesting of mobile networks. This permits an MR to host other MRs in its mobile network. With nested mobile networks, the use of NEMO further amplifies the sub-optimality listed above.

In IETF, the issues of Route Optimization of NEMO are addressed in [rfc4888] and the solution space is analyzed in [rfc4889]. Requirements of Route Optimization in various scenarios are described for networks for vehicles [draft-ietf-mext-nemo-ro-automotive-req] and aeronautic environments [rfc5522]. The proposed solutions for Route optimization are analyzed in section 3.6.

3.5.6 MANEMO

Both MANET and NEMO are designed independently as Layer 3 technologies. NEMO is designed to provide global connectivity and MANET to provide direct route in local area network. **MANEMO** that is the concept of using both MANET and NEMO together could bring benefits of route optimization.

Since direct routes are available in MANET local networks, MANET can provide direct paths between vehicles. These paths are optimized and free from the NEMO tunnel overhead [Tsukada2008, Wakikawa2005a, Lorchat2006d]. The possible topology configuration with MANEMO is described in [draft-wakikawa-manemoarch] and issues and requirements are summarized in [draft-wakikawa-manemo-problem-statement]. In addition, MANEMO are

[1] http://software.nautilus6.org/NEPL-UMIP/

used for vehicle communication, for example, VARON [Bernardos2007] focuses on NEMO route optimization using MANET. It also provides the same level of security as the current Internet even if the communication is done via the MANET route.

3.6 Solution analysis for Route Optimization

There are several propositions for Route Optimization in NEMO context. They cover a broad range of topics in terms of scenarios, benefits and disadvantages. Thus this section describes comparison of multiple approaches. First scenario is described, and then the approaches are classified into five types. Last of all, these approaches are compared. Summary is shown at Table 3.5.

3.6.1 Taxonomy

In NEMO context, Route Optimization is divided into two scenarios that are **Non-Nested Scenario** and **Nested Scenario**. In Non-nested scenario, the issues that are similar in Mobile IPv6 tend to be focused, such as Longer Route, Packet Encapsulation and Bottleneck in the HA that are shown in Section 3.5.5. On the other hand, in Nested Scenario, the focus is on the issues, which do not appear in Mobile IPv6 but NEMO. This is because Nested Mobile Network further amplifies the issues listed above in Non-Nested Scenario.

In Non-nested scenario, there are two approaches from the way to optimize the route. Both approaches have common idea that the Binding Cache is transplanted to a router closer to Correspondent Nodes. "(a) Binding Management on CE" is the Binding Cache is transplanted to Correspondent Entities. On the other hand, in "(b) Infrastructure-based RO", it is transplanted to the nearer HA from the MR. In nested scenario, Some of the HAs are skipped by the solutions. One approach is to use topological Care-of Address that is classified to "(e) Topological CoA relay". The other approaches which aim nested scenario are classified to "(d) Halfway Home Agents Skip". "(c) RO using MANET" is only one approach to aim to both of the two scenarios.

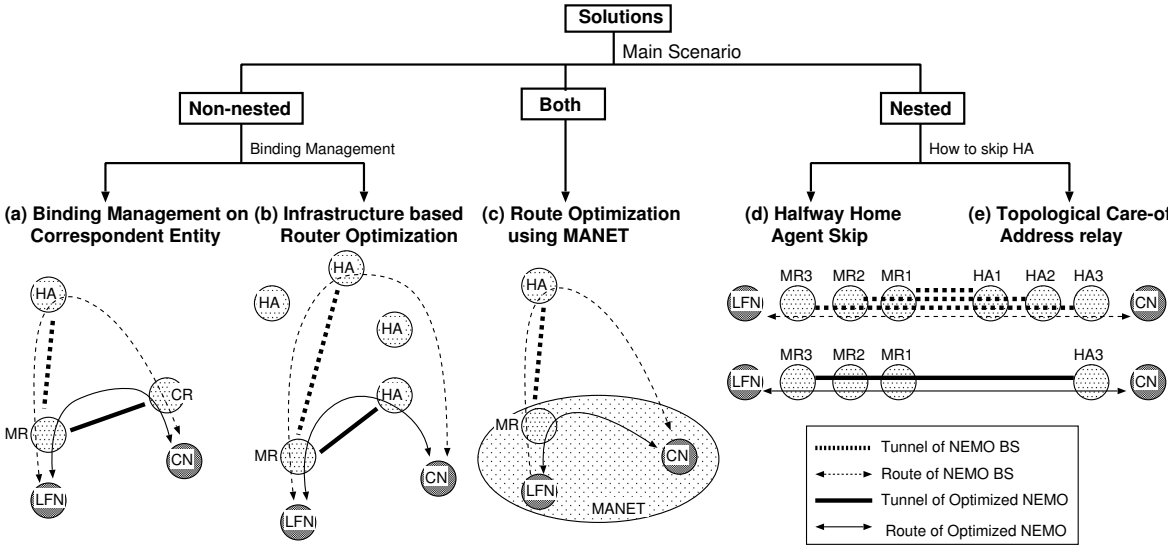


Figure 3.9: Approaches of Route Optimization

Table 3.5: Relation with target scenario and each approach

Main scenario	Approach	(1)	(2)	(3)	(4)
Non-nested	(a) Binding Management on CE	◯	×	◯	×
	(b) Infrastructure-based RO	◯	×	◯	×
Both	(c) RO using MANET	◯	◯	◯	◯
Nested	(d) Halfway Home Agent Skip	×[2]	×[2]	×[2]	◯
	(e) Topological CoA relay	×[2]	×[2]	×[2]	◯

(1) Longer Route (2) Packet Encapsulation
(3) Bottleneck in the Home Agent (4) Nested Mobile Networks

3.6.2 Binding Management on Correspondent Entity

An orthodox approach to Route Optimization in NEMO is for the MR to attempt Route Optimization with a Correspondent Entity as (a) in Figure 3.9. The Correspondent Entity, having received the Binding Update, can then set up a bi-directional tunnel with the MR at the current Care-of Address of the MR. This approach is similar idea with Route Optimization in Mobile IPv6 that Binding Cache management functionality is transplanted from the HA to Correspondent Entity.

[Wakikawa2003, draft-na-nemo-path-control-header, draft-bernardos-mext-nemo-ro-cr] are examples of this approach. They mainly focus on Non-nested scenario, thus issue may still remain in Nested Scenario. [draft-wakikawa-mext-cr-consideration] further investigated for the approach. [Watari2006] focuses both of Non-nested and nested scenario by assuming existence of the local routing protocol within nested mobile networks. The main idea of this proposal must be classified to Binding Management on Correspondent Entity.

Since Correspondent Entity assumes to be closer to the Correspondent Node than the HA, Longer Route is optimized. And Bottleneck in the HA is solved, because the tunnel is created between the MR and the Correspondent Entity instead of the HA. On the other hand, Packet Encapsulation issue is still untouched.

3.6.3 Infrastructure-based Route Optimization

Infrastructure-based Route Optimization is a type of approach that transplants Binding Cache management functionality to a router close to the Correspondent Node instead of the initial HA as (b) in Figure 3.9. One example is to make use of Mobility Anchor Points (MAPs) such as defined in Hierarchical Mobile IPv6 [rfc5380]. Another example is to make use of proxy HA such as defined in the global Home Agent to Home Agent (HAHA) protocol [draft-thubert-nemo-global-haha].

Longer Route is optimized by Binding Cache being managed by closer router such as MAPs or proxy HAs. And Bottleneck in the HA is solved, because the tunnel is created between the MR and another router instead of the initial HA. On the other hand, the Packet Encapsulation issue is still untouched. Nested mobility optimization needs additional scheme to be solved.

[2]Issues are alleviated by reduced tunnel overhead

3.6.4 Route Optimization using MANET

Route Optimization using MANET is the approach of local packet delivery in MANET instead of NEMO as (c) in Figure 3.9. In other words, this is the MANEMO case that described in section 3.5.6. The example is [Tsukada2008, Wakikawa2005a, Lorchat2006d]. This assume that both MRs and Correspondent Entity support both of NEMO and MANET technologies and they exchange direct route when they are connecting in same MANET cloud. Thus the path of communication is switched to direct route from non-optimized route, when destination and source of communication are in same MANET cloud.

By using direct route, all the HAs and tunnels are skipped in the both cases of Non-nested and Nested. Thus communication is free from Longer Route, Packet Encapsulation and Bottleneck in the HA in the both cases. However, this optimization can be utilized only in local MANET area. Detailed problem statement was described in [draft-wakikawa-manemoarch, draft-wakikawa-manemo-problem-statement, draft-mccarthy-manemo-configuration-problems] in MANEMO WG [manetwg] in IETF.

3.6.5 Halfway Home Agent Skip

Halfway Home Agents Skip mainly focuses on nested scenario to reduce number of tunnels and number of HAs on the path as (d) in Figure 3.9. Examples are [draft-thubert-nemo-reverse-routing-header, draft-na-nemo-nested-path-info] that the tunnel ends up between MR3 and HA3 by using Reverse Routing Header (RRH) in Figure 3.9. On the other hand, the tunnel is end up between MR1 and HA3 in [draft-ng-nemo-access-router-option]. Those three examples must be classified to Nested Mobility Optimization approach with slight different, because all of them has an idea to skip the some of HAs and the tunnels in Nested mobile network.

By skipping the HAs and tunnels, the performance of a nested mobile network is decreased to almost the same level as NEMO basic support. But some sub-optimality still exists at the same level as NEMO basic support such as Longer Route, Packet Encapsulation and Bottleneck in the HA.

3.6.6 Topological Care-of Address relay

Topological Care-of Address (CoA) relay is mainly focus nested scenario to reduce number of tunnels and number of HAs on the path as (e) in Figure 3.9. This approach is divided into two types that are with Prefix Delegation (PD) [rfc3633] and with NDP [rfc4861] proxy. Former way is for parent MRs to have functionality of Prefix Delegation. Examples of this are [draft-perera-nemo-extended, draft-leekj-nemo-ro-pd]. MRs in nested mobile network acquire its Care-of Address that is from an aggregatable address space starting from the access router by prefix delegation. Since the Care-of Address is routable without both of HA1-MR1 tunnel and HA2-MR2 tunnel, finally only tunnel between MR3 and HA3 is established.

Example of later way with NDP proxy is [draft-jeong-nemo-ro-ndproxy]. An MR relays the prefix of its care-of address to the nodes behind the MR. All MRs in nesting will configure a care-of address from the network prefix advertised by its access router. The entire mobile network and its access network form a logical multi-link subnet, thus eliminating any nesting. In both types in this approach, by skipping the HAs and tunnels, the performance of a nested mobile network is decreased to almost the same level as NEMO basic support. But the same sub-optimality still exists as NEMO basic support such as Longer Route, Packet Encapsulation and Bottleneck in the HA.

Part II

Path Selection in ITS Station Architecture

Chapter 4

Problem statement and Design Requirements

Contents

In this chapter, we present issues and design requirements to optimize the communication between ITS Stations in IP-based cooperative ITS. First, three issues are presented. *Path selection* is a decision-making issue selecting an appropriate path matched with application requirements from the multiple paths exist between vehicle ITS Stations. The path selection process must be performed as the combination of the selections of various parameters (Communication Interface (CI), locator, Access Router (AR), routing and anchor). To allow intelligent path selection, geographic information plays an important role. *Geographic Position Management* is an issue about how to propagate and manage the geographic information in ITS Stations. To combine IPv6 and GeoNetworking, we are facing new *addressing and routing issues*. To realize IPv6 GeoNetworking, we must investigate how the IPv6 packets are delivered over GeoNetworking without *IPv6-awareness* in order not to impact too much the ITS Station reference architecture.

Then, we explain what are the design requirements for the solution. The solution shall follow the ITS Station architecture described in Section 2.2 keeping layers independence. The parameters and messages exchanged between the layers must be flexible and be abstracted as much as possible for future extension. We follow the design concept of ITS Station router and host split where the ITS Station router is in charge of entire station communication and the hosts running applications are freed from the communication management. The IPv6 GeoNetworking solution must support all the new types of geographic routing communications (*e.g.* GeoBroadcast described in Section 3.3.2.2). To support IPv6 GeoNetworking, the GeoNetworking management should be transparent from the ITS Station host running applications. ITS Station must be able to change the point of attachment one link to another without interrupting the ongoing IP sessions. *i.e.* Network Mobility support is needed. The paths must be used according to the application requirements and multiple paths must be used simultaneously.

4.1 Issues

4.1.1 Path Selection

As shown in Figure 4.1, there are different types of paths linking two vehicle ITS Stations:

- **Anchored Path**
  As shown in Section 3.4, the communication path to a mobile node passes via an anchor fixed in the Internet. The anchored path is made of three parts: from the mobile node to the access network, between the anchors and from the anchor to the access network. The parts from the access network to the anchor and from the anchor to the access network must be re-established as the vehicle moves and attaches to a new AR. In this case, certain mobility protocols require the additional encapsulation at packets from access network to anchor and from anchor to access network. NEMO, for instance, leads to an additional 40 bytes header encapsulation that increases packet overhead and increases the risk of packet fragmentation. On the other hand, the part between anchors is free from encapsulation and delivered by normal Internet routing.
  The anchored path leads to communication latency that comes from processing delay in the anchors and from non-optimized path via the anchors. As an anchor supports mobility of the other vehicle ITS Stations, the traffic from these vehicle ITS Station converges in the anchors. This may also cause communication latency because of the network traffic congestion.

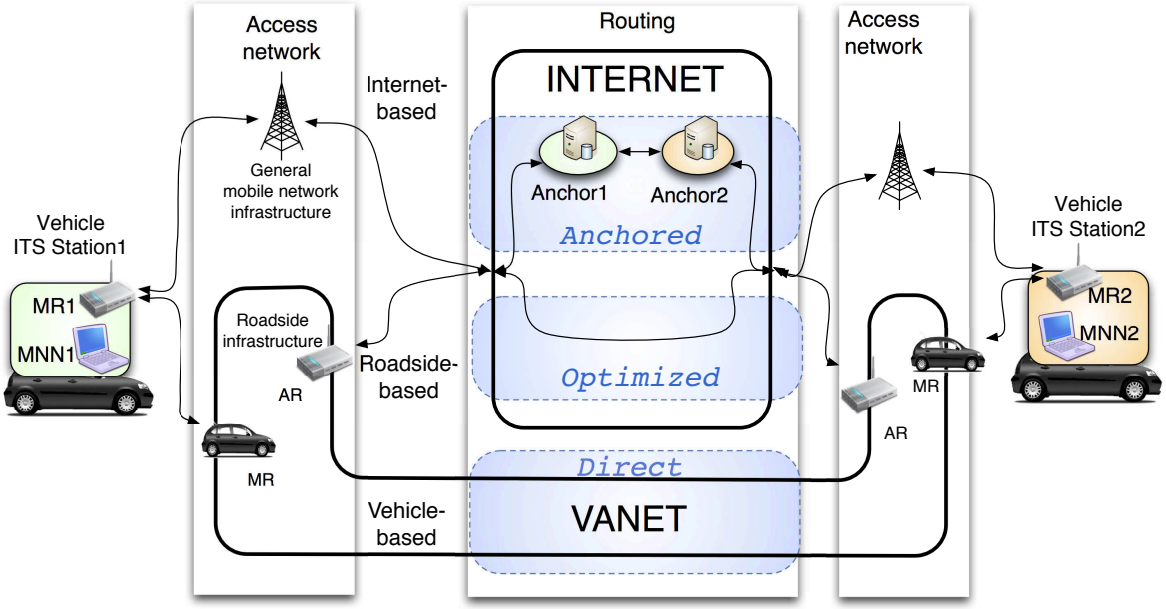


Figure 4.1: Paths between vehicle ITS Station

- **Optimized Path**
  The optimized path is a path that avoids path via the anchors. Thus communication characteristics should be stable and reliable. In the initial state of communication, the packets may be routed via an anchor when vehicle ITS Station supports mobility. Then as a result of Route Optimization at arbitrary time, the optimized path is taken in order to enjoy better network performance i.e. latency and bandwidth. In contrast to the anchored path, the optimized path is free from anchor and packets are routed by normal Internet routing. Using the optimized path, the latency is shortened by avoiding the redundant path portion to the anchors, skipping processing of encapsulation in the anchors and avoiding the traffic congestion near the anchors. On the other hand, there may still remain packet encapsulation even using the optimized path.
  For example in NEMO, non-nested cases of Route Optimization (See Section 3.6) are classified into (a) Binding management on Correspondent Entity (CE) and (b) Infrastructure-based Route Optimization . The tunnel is directly established between MRs with solution class (a). In this case, packets between vehicle ITS Stations take the optimized path. On the other hand, the tunnel is established with the nearest anchor in class (b). This category of solutions does not skip anchors. Thus the path is categorized as anchored path, even if Route Optimization is applied.
  As seen in NEMO Route Optimization solution class (a), the packets taking the optimized path may be encapsulated with additional header as much as on the anchored path.

- **Direct Path**
  Direct path between vehicles can be made by ad-hoc routing without passing through any infrastructure. We refer to this as "vehicle-based" communication (See Section 2.2.3). To enable direct path between vehicles, the vehicle ITS Stations must exchange the routes each other. Direct path is usually available in a limited geographic area because the propagation of the paths is limited in a VANET.

Direct path is completely free from suboptimal path via anchors and from any mobility support tunnel encapsulation.

The link between MR to an AR is a wireless link that usually has long latency and low bandwidth. The wireless link is unstable because vehicles are moving and hoping from AR to AR. Thus the link often becomes the bottleneck of communication between different vehicle ITS Stations. The communication characteristics in the access network are determined by the communication interface selection and the access router selection. First, in some cases, selecting a path is equivalent to selecting a communication interface, because the access router is determined consequently. Also, many factors in the access network depend on the media type of communication interface including data rate, cost, reliability, security, power consumption, and etc. Second, the selection of a path depends on the selection of the access router, because paths can be considered as different when an interface connects to different access routers. The selection of the access router is important especially in a VANET environment where multiple ARs may be reached in a multi-hop manner.

The four portions of paths between vehicle ITS Stations must be considered for selecting the path. For the access network part, it is important to perform communication interface selection and access router selection. Anchored path requires the selection of anchors and optimized path requires the selection of Route Optimization method.

In other words, the path selection process must consider:

- Types of path
- Communication interface
- Locator
- Access router
- Routing
- Anchor

We need to investigate which parameters are important in the path selection decision-making process. In addition, we need to investigate how a path that is suitable according to application requirements can be selected.

4.1.2 Geographic Position Management

The path selection decision is made according to various parameters as discussed in Section 4.1.1. The parameters are divided into static parameters and dynamic parameters. For example, media type, cost, reliability and security of communication are static parameters set up at boot time. On the other hand, data rate and delay are dynamic parameters because they change frequently depending on the network conditions (vehicle speed, radio signal propagation, density of vehicle, weather and etc.).

While pre-configured values could be used for static parameters, real-time measurement are needed to obtain dynamic parameters. However the measurement of dynamic parameters (*i.e.* delay and data rate) is not always easy. Thus the most frequently used way to evaluate the quality of access network is to measure the Received Signal Strength Indication (RSSI) on the egress interfaces of the MR. RSSI can be used for both communication selection and access router selection, if it can be obtained. However RSSI is not available in the VANET,

and even all the link evaluation schemes are not useful in ad-hoc routing because the first hop link quality does not reflect the entire path in the multi-hop network.

In vehicular multi-hop networks, other metrics are necessary to evaluate the link quality. Geographic metric are suitable to evaluate the link thanks to the GPS equipment deployed in each ITS Station. Example of geographic parameters are shown below:

- Distance,
- Movement speed, and
- Movement direction

To calculate the distance between two ITS Stations, the position of the two ITS Station is necessary. Assuming that an MR is equipped with a GPS device and can get its position directly from the device, the MR should obtain the position of the other ITS Station for the calculation of distance, and vice versa. Movement speed and movement direction have to be exchanged as well. Hence it is important to exchange geographical information between ITS Stations.

We need to investigate what information is necessary, how ITS Stations can exchange the geographic information, and how ITS Station can manage the information. In addition, we have to investigate how the decision-making algorithm can treat geographic metric for the decision.

4.1.3 Addressing and Routing in IPv6 GeoNetworking

IPv6 is needed for Internet-based communication mode whereas GeoNetworking is necessary for vehicle-based and roadside-based communication modes. IPv6 and GeoNetworking must thus be combined. However, we are facing new addressing and routing issues.

Following IPv6 addressing, any node is required to obtain a topologically correct address on the link on which it is currently attached to. On the other hand, the addressing scheme of GeoNetworking is simple. Any node can obtain its geographic position expressed in World Geodetic System 84 (WGS-84) from certain positioning devices. *e.g.* GPS. We must investigate how IPv6 address and geographic position expressed in WGS-84 are mapped.

IPv6 routing is based on the longest match principle. Each node forwarding packets examines all routing table entries by the destination address and chooses the path that matches longest bits. GeoNetworking routing, on the other hand, is based on the greedy forwarding scheme where each node forwards the packet to the nearest neighbor node to the destination geographic position. We must investigate how the source GeoNetworking node can find the geographical location information of the destination or GeoNetworking ID from IPv6 packet

4.1.4 IPv6-Awareness in GeoNetworking

IPv6 packets cannot be routed over a GeoNetworking link, because the GeoNetworking routing algorithm requires the geographical location information of the destination to route the packet. Otherwise, it needs the destination GeoNetworking ID to request the destination geographical location information to the neighbor nodes using location service.

Since we are targeting IP-based cooperative ITS applications, it is logical to make the source and destination GeoNetworking nodes IPv6 aware. However the intermediate nodes

the multi-hop V2V path may not be aware of IPv6, because nodes only supporting GeoNetworking may be deployed. If we force all the nodes to be both IPv6 and GeoNetworking-aware nodes to enable IPv6 communication over GeoNetworking, it would impact too much the ITS Station reference architecture. We shall limit the IPv6 GeoNetworking functionality on the source and the destination GeoNetworking nodes running application requiring IPv6.

We need to investigate how GeoNetworking can be made IPv6-aware. Moreover, we have to investigate how intermediate GeoNetworking nodes can deliver IPv6 packets over the GeoNetworking link without IPv6 awareness

4.2 Design Requirements

4.2.1 Layers Independence

As described in Section 4.1.1, the decision for path selection should take into consideration information from the several layers. In order to address the issues discussed in Section 4.1.1, a decision making mechanism that respects the layered architecture separation of the layers is needed.

The path selection mechanism shall preserve the layer independence of the ITS Station architecture. The ITS Station architecture follows a layered structure where each layer is independent from the other layers. The advantage of such layered architecture is that applications do not need to be aware of the available wireless technologies at the access layer and network protocols that establish the communication from the source to destinations. The other layer can handle the access layer and the network layer technologies without involving the technology specific functions.

4.2.2 Abstraction and Long-Term Architecture

The path selection shall be designed in the most possible abstracted way. This will work the decision-making mechanism more extensible and flexible to accommodate the progressive development of ITS. At the network layer, there are various modules such as IP, non-IP, GeoNetworking and etc, and more modules must appear in the future. Also, for example in IP, the functions (NDP, DHCP, NEMO, MNPP and etc.) may be modified, improved or replaced in the future. For instance, it is good at the management entity not to assume a particular protocol at the network layer to provide L3 session continuity, currently this is offered from NEMO in [ISO-21210:2011-CALM-IPv6], but could be replaced *e.g.* by Proxy Mobile IPv6 (PMIP).

4.2.3 ITS Station Router and Host Split

As described in Section 2.2.3, ITS Station consists of router(s) which is in charge of the communication of the entire ITS Station and hosts running applications. In this concept, the ITS Station hosts are free from managing the communication beyond the link where the hosts connect to, since the router is responsible for managing the communication of the entire ITS Station. To solve the issues presented in Section 4.1, the solution must not break the design concept to keep this benefit, although GeoNetworking, originally, does not support the split of functions between router and host.

4.2.4 GeoNetworking Communication Type Support

GeoNetworking defines four types of communications:

- GeoUnicast,
- GeoBroadcast,
- GeoAnycast and
- TopoBroadcast

The first three types are geographic routing and the other one is topological routing. From the point of view of endpoints, GeoUnicast and GeoAnycast are point-to-point communication types and GeoBroadcast and TopoBroadcast are point-to-multipoints communication type (See Section 3.3.2.2 for more details). The solution shall support these four types of communication.

4.2.5 GeoNetworking Transparency for Hosts

To enable geographic routing, GeoNetworking nodes obtain the geographic coordinate from a GPS device and exchange the geographic location to their neighbors using beaconing and location service. The geographic location of neighbor nodes is managed in a location table in each GeoNetworking node.

In the ITS Station architecture, the ITS Station router is responsible for the communication while hosts run applications. As such it is not favorable that all the nodes in the vehicle support the basic messaging of GeoNetworking and location table management. Because some hosts *e.g.* sensor node may have very limited computing resource. More crucially, not all of hosts have GPS device, since some of them may be temporally brought to the vehicle. *i.e.* PDA, music player, PC and etc. A node in the vehicle should thus support GeoNetworking on behalf of the other nodes in the same ITS Station internal network.

Thus, as a design point of view, GeoNetworking management of the vehicle ITS Station is better seen as the ITS Station router's responsibility and should be transparent to the hosts. The hosts should better have not responsibility in GeoNetworking management.

On the other hand, some Geo-aware applications may need to specify the geographic destination area where packets shall be transmitted to. In this case, the host must be able to indicate the geographic area where the packet shall be transmitted that requiring any new function at the network layer.

4.2.6 Network Mobility Support

IPv6 GeoNetworking shall support both of vehicle-based and roadside-based communication. In roadside-based and Internet-based communication case, MNN should be accessible from CN in the Internet and be able to communicate with any CN in the Internet. Internet connectivity is provided through MR via any wireless media either with GeoNetworking or without GeoNetworking. To provide on-the-move and uninterrupted Internet connectivity, NEMO as specified by the IETF is recommended in the ISO TC204 WG16 standard [ISO-21210:2011-CALM-IPv6]. Hence, IPv6 GeoNetworking shall support NEMO.

4.2.7 Simultaneous Usage of Paths

As we discussed in Section 4.1.1, there could exist multiple paths between two neighbor ITS Stations. Simultaneous usage of multiple paths provides the user or the application better performance and more reliability by distributing the packets into multiple paths. Multiple interfaces connected to different links can increase the total available bandwidth. Moreover, multiple paths can decrease latency by avoiding of network congestion.

4.3 Conclusion

In this Chapter, we presented issues and design requirements to optimize the communication between ITS Stations in IP-based cooperative ITS. Table shows 4.1 shows the issues and the design requirements with three topics (ITS Station Architecture, Mobility Enhancement, and IPv6 GeoNetworking) even through they are somehow linked. We must design the solutions for the three topics based on the issues and the requirements arisen in this Chapter.

	ITS Station Architecture	Mobility Enhancement	IPv6 GeoNetworking
Issues	• Geographic Position Management	• Path Selection	• Addressing and Routing in IPv6 GeoNetworking • IPv6-Awareness in GeoNetworking
Requirements	• Layers Independence • Abstraction and Long-Term Architecture • ITS Station Router and Host Split	• Network Mobility Support • Simultaneous Usage of paths	• GeoNetworking Communication Type Support • GeoNetworking Transparency for Hosts

Table 4.1: Issues and Requirements

Chapter 5

Solution Design

Contents

In this chapter, we present our approach in designing our solution to the problem expressed in the previous chapter, and in accordance with the design requirements. In order to optimize the communication between ITS Stations in IP-based cooperative ITS, we need to address the following six questions: What is the fundamental information required by the ITS Station Management Entity (SME), where the information comes from, which information is maintained in the network layer, how the network information is provided to the SME, how the path is selected and how IPv6 and GeoNetworking are combined. To answer these questions, we investigate how the network layer parameters are abstracted in the management entity and how the parameters are transmitted between the SME and the network layer. The investigation leads us to define three tables in the SME, the ITS Station information table, the path information table and the flow requirement table. We also figure out that four primitives are required for the interaction between the SME and the network layer. Two of them are needed to instruct the network layer to route flows to a given path and correspond to the primitives already defined in ISO specifications (*MN-REQUEST* and *MN-COMMAND*) for a network layer protocol block other than IPv6, whereas two new ones are needed to access to the information contained in the Management Information Bases (MIB) already defined in the network layer IPv6 protocol blocks. An adaptation agent is needed in the IPv6 protocol block in order to exchange the information with the SME and to process instructions coming from the SME. We then investigate how the best path is selected. The path selection decision is performed in the SME according to the application requirements recorded in the flow requirement table and the network status and interface information recorded in the path information table. It is important for intelligent path selection to predict the candidate path and its characteristics. The prediction performed in the SME is stored in the path information table. Finally, We investigate how IPv6 and GeoNetworking are combined. The IPv6 packets are encapsulated into GeoNetworking packets in the ITS Station router which is responsible for communication of the entire ITS Station and is managing GeoNetworking transparently to the ITS station hosts. A network-layer internal interface is needed to transmit packets between IPv6 and GeoNetworking (GeoIP SAP). As a result of this investigation, an abstraction model for management and network interaction is presented. Finally, we conclude this chapter by showing how the three major contributions *i.e.* the path selection manager, the interaction between the SME and the network layer (MN-SAP) and IPv6 GeoNetworking mechanisms are going to be presented in the following chapters.

5.1 Approaches to the Solutions

Figure 5.1 gives the overview of our proposed architecture. The **path selection manager** located in the management entity makes a decision based on the information from all the layers. This study mostly focuses on the interaction between the management entity and the network layer **(MN-SAP)**. From the design requirements in Chapter 4, the decision in the management entity is taken based on abstracted parameters not bound to a particular protocol and technologies. To make the management parameters abstracted, we need to define the abstracted messages and the parameter exchanged via the interface between the management entity and the network layer. We also focus the interface between IP and GeoNetworking (**GeoIP-SAP**) to combine these protocols.

There are several protocol blocks in the network layer (*e.g.* IPv6, GeoNetworking, FAST and etc.). In order to abstract the protocol blocks from the view point of the ITS Station management entity, we need to clarify what is the fundamental information, types of network

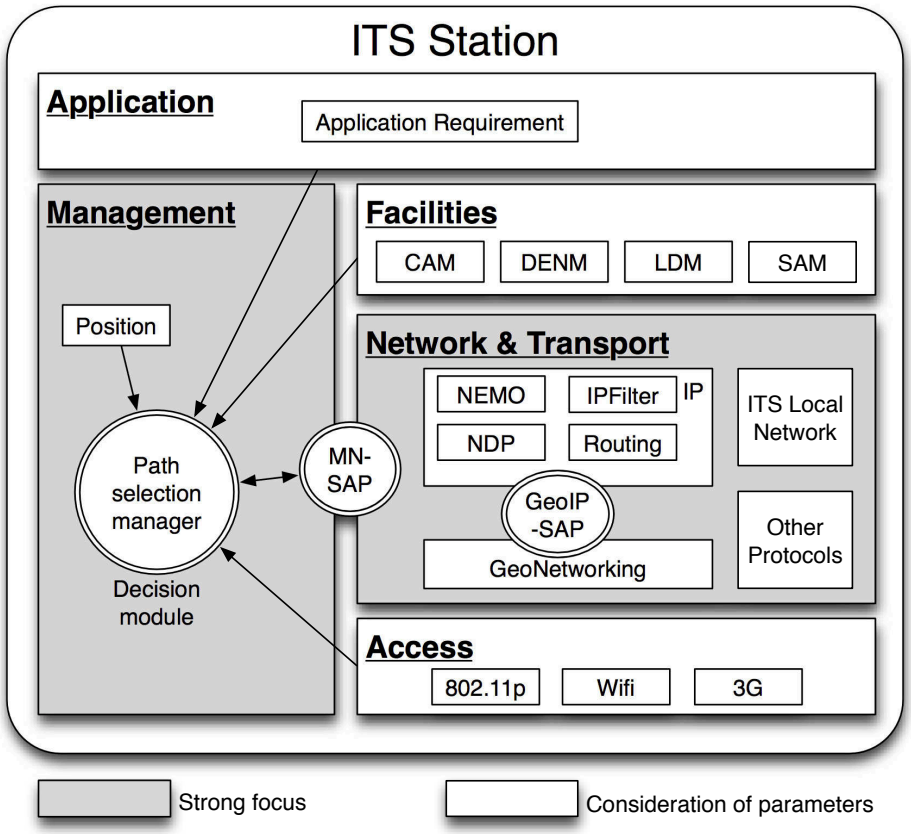


Figure 5.1: Overview of Proposed Architecture

information and how to pass them to the management entity. We also need to investigate how the path selection decision is taken based on provided network information, and how IPv6 and GeoNetworking are used together to take the advantage of these protocols.

Hence, we need to answer the following questions.

- What is the fundamental information required by the management entity?
- Where the information comes from?
- Which information is maintained in the network layer?
- How the network information is provided to the management entity?
- How path is selected?
- How IPv6 and GeoNetworking are combined?

The following sections discuss about each topic.

5.1.1 What is the Fundamental Information Required by the Management Entity?

Following the existing ISO specifications, the management entity has the information about VCI/CI and self ITS Station's position. Based on this information, the management entity

is able to make a decision for CI selection. However other information for path selection is missing. There are:

- Network topology information,
- Access router information,
- Routing information,
- Anchor information

Thus we need to provide the management entity with parameters related to network status so that the path selection manager could make a good decision.

Regarding MN-REQUESTs and MN-COMMANDs, current ISO specifications provide the means to transmit the information between the management entity and the forwarding table (See Appendix C). However the information recorded in the forwarding table is not enough to make an intelligent decision for path selection. For path selection, the management entity should be able to access more network status information and it should transmit the decision to the network protocol blocks, not directly to the forwarding table.

To enable intelligent path selection, MN-REQUEST and MN-COMMAND must transmit the following information between the management entity and the network layer.

- Topological locator of ITS Stations (*e.g.* IP address),
- Geographic information of ITS Stations (*e.g.* Position, direction and speed),
- Node information (*e.g.* anchor, MR, AR),
- Capability (*e.g.* Mobility support, GeoNetworking support),
- Network performance related information (*e.g.* delay, payload size, etc),
- Network layer service (*e.g.* DHCP, SLAAC, Multicast, etc),
- Reachability (*e.g.* On-link, VANET, global), and etc.

In this section, we consider the fundamental network layer information that is required by the ITS Station management entity.

As the vehicle ITS Station moves more dynamically than the other ITS Stations, the network around vehicle ITS Station needs the most information in each network layer protocol blocks. Thus we focus on the inputs to the SME in vehicle ITS Station. The information required in the other types of ITS Stations should be a subset of the vehicle ITS Station.

First of all, a network consists of *nodes* (or *vertices*) and *links* (or *edges*). The vehicle ITS station should be aware about the surrounding ITS Stations (*nodes*) in order to comprehend the status of the network around it. Especially, the SME should be aware about the surrounding ITS Stations and the role they play (vehicle ITS Station able to relay information to other vehicle, and roadside ITS Station providing Internet connectivity, etc.) This is essential role for determining appropriate path where to route the packets.

We name the set of information about ITS Stations as **ITS Station Information** and define that the management entity stores the information of neighbor ITS Stations in the database named **ITS Station Information Table**.

On the other hand, path information is also important to comprehend the network status. We define that **Path Information** as the information of a set of connected *links* (or *edges*)

to the destination. The SME stores all the possible paths' path information in the **Path Information Table**.

In addition to the two tables, the SME needs the **Flow requirement** to perform the path selection decision. The Flow requirement must have the information about which flow needs to satisfy what network performance requirements. Similar concept is found in [ISO-24102-1-ITSS-management] as the *application requirements list* (*ApplReqList*). However current *ApplreqList* is designed to enable the CI selection (shown in Appendix C). Thus we need to define the flow requirement to adapt for the path selection. A set of flow requirement must be recorded in the management entity as **Flow requirement table**.

Based on the ITS Station information table and the path information table, the SME comprehends the network status. The path selection decision must be taken by matching the network status in the application requirements in the flow requirement table.

5.1.2 Where the information comes from?

The three information tables (described in Section 5.1.1) recorded in the management entity comes from following three sources.

- **Data plane (*e.g.* access, network, facilities layers)**
  Some information comes from the data plane via the interfaces defined between the management entity and the layers. The CI information comes from the access layer. The network information (topological locator, geographic position, etc) of the neighbor ITS Station can be obtained in the network layer as a result of the signalling exchange between ITS Stations in various network layer protocol blocks. The network information is sent to the management entity via the Management-Network interface. The geographic position of the ITS Station can be provided also from the facilities layer, that is originally obtained by the message exchange of CAM. The application requirements comes from the facilities layer, for example, application requirements for CI selection is transmitted by the command defined as "*ITS-S-Appl-Reg*" in [ISO-24102-CALM-Management].

- **Input devices (*e.g.* computer vision, reading media, maps download)**
  The management entity can obtain the neighbor ITS Station information from the input from the devices installed in the ITS Station. For example, the computer vision using video camera or radar equipped in the vehicle ITS Station can detect a neighbor ITS Station's geographic position. Or, an operator distributes the geographic position and the topological locator of the roadside ITS Station via media (*e.g.* DVD-ROM). Or even such information can be available by downloading the map data.

- **Calculation (*e.g.* statistical way, mobility model)**
  The management entity can compute neighbor ITS Station information (*e.g.* topological locator and geographic position of ITS Station) by statistical way in the history, when the vehicle is on the way of everyday's trajectory. When a vehicle ITS Station can discover certain roadside ITS Station every days at same position, it can be recognized that it is fixed at the point. The availability of access network via such roadside ITS Station can be calculated using mobility model of the vehicle (*i.e.* trajectory prediction).

These obtained information should be recorded in the ITS Station information table, Path information table and flow requirement table.

5.1.3 Which Information Is Maintained In The Network Layer?

The following list shows examples of the "actions" performed in each protocol block. Messages are sent in order to discover neighbor nodes or services, notify information, etc, when it is necessary.

- IPv6
  - Neighbor Solicitation, Neighbor Advertisement, Router Solicitation, Router Advertisement and ICMP redirect (NDP)
  - MNPP solicitation and MNPP advertisement (Mobile Network Prefix Provisioning (MNPP))
  - Solicit, Advertise, Request, Confirm, Renew, Release and etc (DHCP)
  - Binding Update, Binding Acknowledgement, DHAAD request and DHAAD reply (NEMO)
- GeoNetworking
  - Beaconing,
  - location service request, and location service reply
- FAST
  - Service Advertisement Message and
  - Service Context Message
- Other action in ITS local network and other protocol blocks

The following databases are maintained in each of the ITS Station network and transport protocol blocks. The information collected as a result of these above actions is often stored in the database of each protocol block in the network layer listed bellow:

- IPv6
  - Routing table (IP Routing)
  - Neighbor Cache, Destination Cache, Prefix List and Default Router List (NDP)
  - Filter rule (IP Filter)
  - Binding Update List, Binding Cache, Home Agent List and NEMO prefix List (NEMO)
- GeoNetworking
  - Location table
- FAST
  - Groupcasting Scheduler,
  - *serviceList*,
  - *ipServList* and

  - *servContextList*

- Other database for other protocol blocks

In conclusion, each network layer protocol block maintains the database that stores the "state" of the network. The management entity must be informed about the network state.

5.1.4 How the Network Information is Provided to the Management Entity?

The network layer is basically independent and autonomous. Each network layer protocol block works without involvement of the other layers. Figure 5.2 shows the circulation between "state" and "action" in the network layer. Each network protocol block has its own database to store the state of the network status. *i.e.* routing table in IP, location table in GeoNetworking and *serviceList* in FAST. Then, once an action is taken, the database is updated as the state changes. The action includes transmission and reception of messages. *i.e.* Neighbor Solicitation, Neighbor Advertisement in IP, beaconing in GeoNetworking, Service Advertisement Message in FAST.

The network layer protocol blocks may have default settings instructing how to behave by default. *i.e.* IPv6 forwarding enabled/disable, default hop limit in IP and default HA in NEMO. In many protocol blocks, the Management Information Base (MIB) defines default actions. The MIBs also provides accessibility to "state" data such as the number of input IP datagrams in IP, maximum sequence number of binding update for NEMO.

Although the network layer works fine without involvement of the SME, the SME can take a more intelligent decision based on the information from all the layers. To enable the involvement of the SME, the network layer protocol blocks should share the "state" with the management entity. Then a decision is taken based on information from all the layers. The SME intervenes the "action" of the network layer protocol blocks based on its decision. Hence, the SME needs to obtain the information about the "state" and intervene the "action" of the network layer protocol blocks.

There are two modes where the SME can obtain the "state" information depending on which entity initiates the message such as:

(1) State Data Acquisition: the SME requests the acquisition of state data of the network layer contained in the MIBs, when the SME needs it (On demand).

(2) Event Notification: the network layer notifies the events that cause the state change, when it happens (On time).

There are also two modes where the SME intervenes the "action" in the network layer protocol blocks depending if the action shall be taken immediately as follows:

(3) Default Action Configuration: the SME updates the default behavior of a network layer protocol block's MIB when it needs (On demand). The network layer protocol block takes an action based on the definition of the default behavior.

(4) Action Request: the SME requests an action to a network layer protocol block based on the decision. The decision is immediately reflected in the network layer (On time).

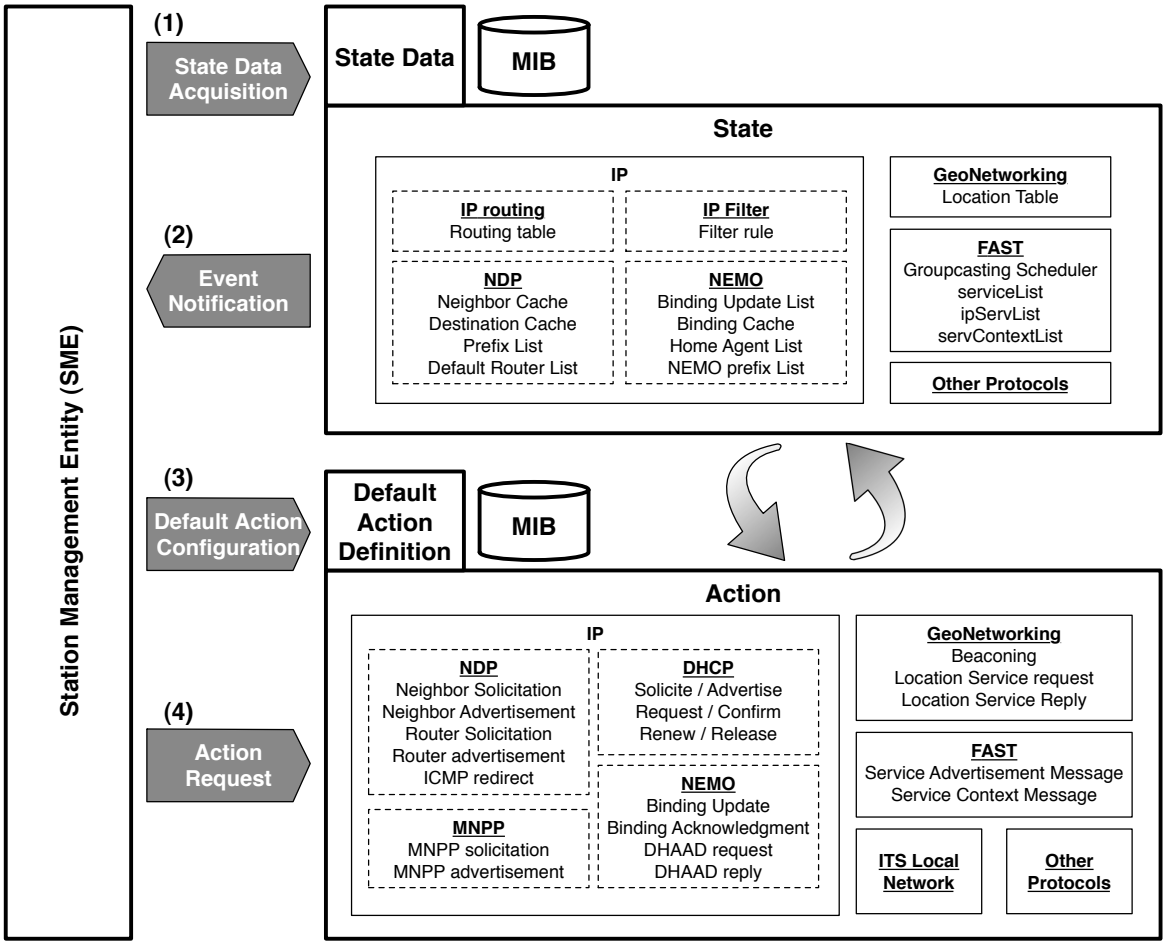


Figure 5.2: Category of Interactions

In the four interactions above, (1) State Data Acquisition and (3) Default Action Configuration can be realized by accessing the MIB of each network layer protocol block that are already well defined and implemented. Thus it is reasonable to reuse them. Since the existing specification of MN-REQUEST and MN-COMMAND does not have primitives to access the MIBs in the network layer, we need to define new primitives.

(2) Event Notification and (4) Action Request corresponds to MN-REQUEST and MN-COMMAND (specified in ISO), respectively.

Table 5.1 summarizes the discussion above.

	Network status notification	Action Instruction
On demand	(1) State Data Acquisition (Access to the MIB)	(3) Default Action Configuration (Access to the MIB)
On time	(2) Event Notification (MN-REQUEST)	(4) Action Request (MN-COMMAND)

Table 5.1: Category of Interactions

We also need to define the interaction between SME and the network layer in the most abstracted way as possible in order to fulfill the design requirements described in Section

4.2.2. Details are provided in Chapter 7.

The interaction between the ITS Station management entity and the ITS Station network and transport layer is illustrated in Figure 5.3. From the network layer to the SME , the network status in the network layer is notified so that the SME can make appropriate decision. Then from the management entity to the network layer, the SME sends the instructions to the network layer where they are interpreted by an adaptation agent that translates and passes these instructions to the appropriate module (set of protocols).

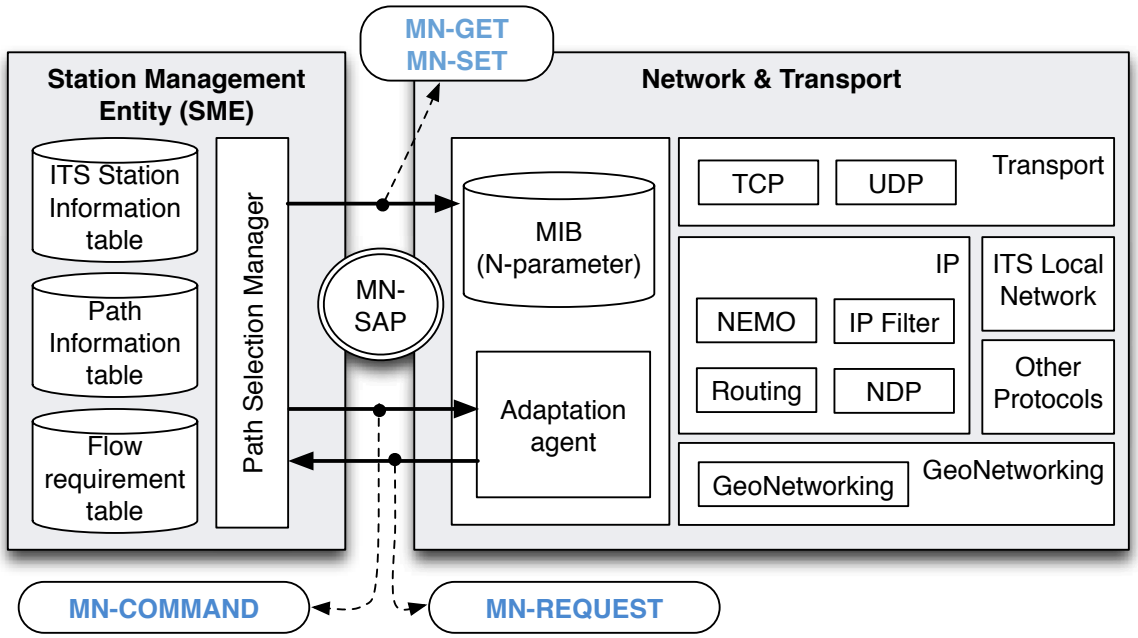


Figure 5.3: Interface Between Management Entity and Network Layer

There are two types of communication modes for both network status notification from the network layer to the SME and instruction from the SME to the network layer. The network status notification has two communication modes. First one is issued from the network layer to the SME to notify an event happens in the network layer (*MN-REQUEST*). The other one is issued by the SME to the network layer to read the values of MIB (defined as N-Parameter in Section 7.1.1) updated regularly by the network layer (*MN-GET*). The action instruction also has two modes: both of them are issued by the SME to the network layer. First type of instruction is translated directly into an action in the network layer (*MN-COMMAND*). The other one sets values of N-Parameter that defines default behavior of the network layer behavior (*MN-SET*). These instructions are defined in Chapter 7.

5.1.5 How Path Is Selected?

First, selecting a path is essentially the matching between the application requirements and characteristics of the paths. The decision body should locate in the management entity in order to take all the layer information into account. We assume the management entity has the application requirements list provided from the facilities layer following the ISO specifications (This is detailed in Appendix C). The characteristics of the paths are also stored in the path information table. Thus the path selection manager can make decisions based on the list and the table in the management entity. The decision shall be taken by

multiple criteria (*e.g.* not only single criteria of delay, bandwidth or stability).

Second, the path information table provides the most up-to-date status of the paths by the notification of the network layer. However, it is important for intelligent path selection to predict the candidate path and its characteristics. The prediction can be performed with, for example, the help of statistical analysis, cross-layer information, information from equipped device and etc. The prediction includes:

- Estimation of the path characteristics (*e.g.* path is "going to down", and "going to up")
- Discovery of candidate path that is not established yet, but theoretically possible

The management entity must maintain following two types of path information so that the path selection manager makes decision based on both of the most up-to-date status and the prediction.

***Available path*:** Path that is established and ready-to-use.

***Candidate path*:** Path that is theoretically possible but not ready-to-use. *Candidate paths* are calculated in the management entity.

The both types of paths information is kept in the path information table with the distinction of the types of the paths.

5.1.6 How IPv6 and GeoNetworking Are Combined?

First, to deliver IPv6 packets over the VANET maintained by GeoNetworking without IPv6 awareness of intermediate nodes (the design requirement detailed in Section 4.1.4), the tunnel technique is used, that is an orthodox approach to avoid awareness of specific technology. For IPv6 GeoNetworking, the IPv6 packets are encapsulated by a GeoNetworking header in order to avoid IPv6 awareness at the intermediate GeoNetworking nodes.

Second, the ITS Station router must be in charge of the GeoNetworking header encapsulation in order to provide the GeoNetwork management transparency for the ITS Station routers (the design requirement detailed in Section 4.2.5).

Third, the GeoNetworking layer can be considered as a sub-layer of the IPv6 layer, when the GeoNetworking header encapsulates IPv6 packet (This is same relation between the access layer and the IPv6 layer. In this case, an access layer protocol header encapsulates the IPv6 packet). Thus we take an approach that the IPv6 layer can treat the GeoNetworking layer similar way as the access layer. In implementation level of the IPv6 forwarding, it is desirable to realize GeoNetworking as communication interface (*e.g.* eth0, ath0) just like the access layer.

5.2 Abstraction Model for Management-Network Interaction

Figure 5.4 shows the abstraction model of Management-Network Interaction. We figure out that two more modes of interaction to the MIB are necessary to reuse the accessibility of network protocol blocks' default action definition and state data, besides MN-REQUESTs and MN-COMMANDs (See Section 5.1.4 for details). By reading and writing the objects of the MIBs, the SME can obtain the state and statistics of the network layer protocol blocks, and modify the default behavior of the protocol blocks. Since the existing specification does not have primitives to access the MIBs in network layer, we need to newly define the primitives (This leads us to define MN-GET and MN-SET detailed in Section 7.1).

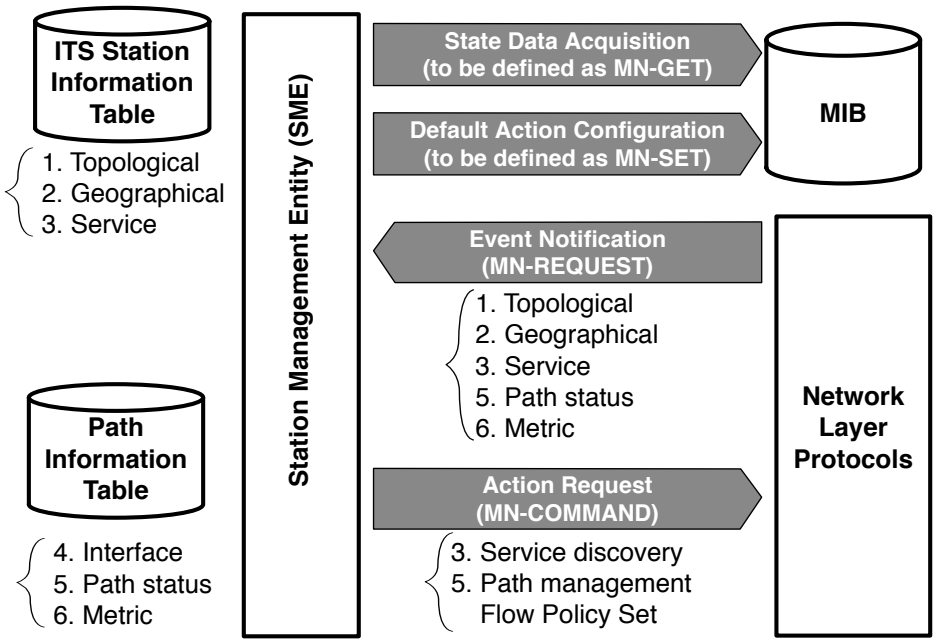


Figure 5.4: Abstraction Model

The management entity has two databases: ITS Station information table and path information table. Both databases have three sub categories. ITS Station information table keeps the (1) topological, (2) geographic and (3) service information of all the neighbor ITS Stations. Path information table maintains (4) CI, (5) path status and (6) metric information of all the possible path at the moment. The path selection manager selects a path in the path information table.

All the sub-category information is sent to the SME using MN-REQUEST except for (5) CI information. Note that the CI information is provided via MI-REQUEST. As ITS Station table is up-to-dated by MN-REQUEST, the management entity is aware where neighbor ITS Station topologically and geographically locates, and which ITS Station can provide which service. Path information table is up-to-dated by MI-REQUEST and MN-REQUESTs as well, the management entity have all the possible paths information with the status and metric of the path.

If the path selection manager finds a path that satisfies the application demand already in the path information table, it sets the flow policy to route the flow to desired path. Otherwise, there are two kinds of commands from the SME to the network layer protocol blocks that are:

Service Discovery: When the path selection manager needs to find other ITS Station that can provide a specific service, the SME requests the service discovery to correspondent network layer protocol block with an MN-COMMAND. *i.e.* "access" and "anchor" are the services related to path selection.

Path Management: When the path selection manager does not find the path that satisfies an application demand, the SME requests the establishment of the path that satisfies the application demand. The decision for CI selection, address selection, access router selection, routing selection, and anchor selection are reflected with the MN-COMMAND.

The four types of interaction between the management entity and the network layer are performed asynchronously. Both side can initiate the interaction in arbitrary time.

5.3 Contributions and Structure of the Following Chapters

Figure 5.5 provides an overview of the architecture and illustrates the three major contributions of this thesis. The following three chapters are organized as below.

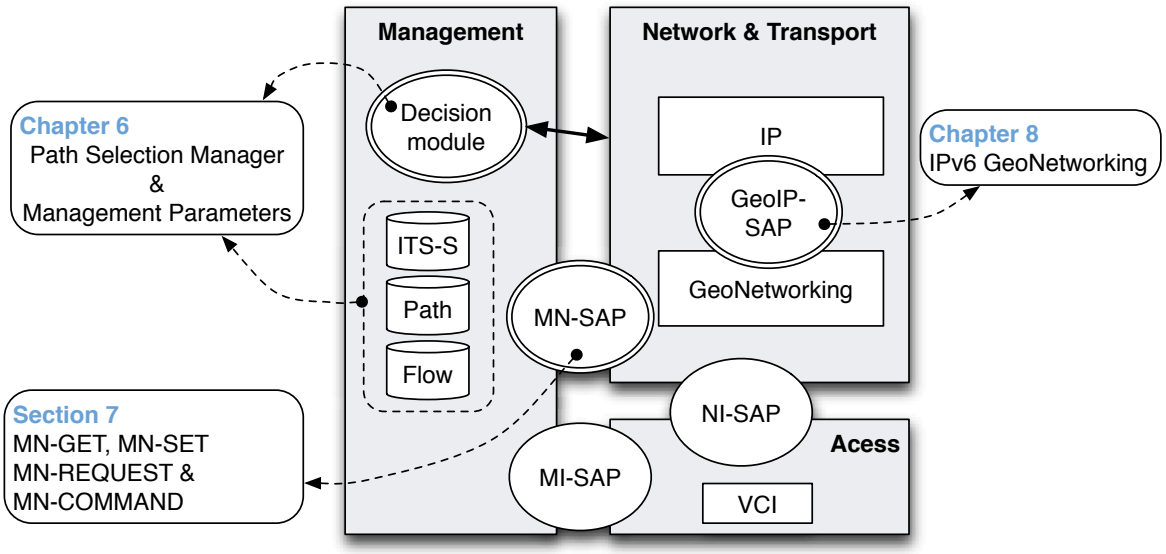


Figure 5.5: Overview of the Contributions

- First, we propose path selection based on cross-layer interaction. The decision module, called path selection manager locates in the management entity in the ITS Station architecture. We define two principal databases in order that the path selection manager makes decision based on the information collected in these databases. The details about the database, parameters, calculation and decision algorithms are described in Chapter 6.

- Second, we define messages and parameters for interaction between the network layer and the management entity as abstracted as possible in order to eliminate the complexity of mixture of protocols blocks in the network layer as described in the previous section. This work extends the existing the interface between the management entity and the network and transport layer (MN-SAP, Management-Network Service Access Point). The details about message format and parameters are described in Chapter 7.

- Third, we propose IPv6 GeoNetworking in order to combine IPv6 and GeoNetworking. IPv6 GeoNetworking provides geographic routing function to IPv6 without adding any function to the hosts that runs IPv6 application. To translate the IPv6 packet into GeoNetworking in MR, we define Geo-IP SAP that is designed as a layer-internal SAP in the ITS Station network and transport layer. The details are described in Chapter 8.

Chapter 6

Path Selection Manager

Contents

In this chapter, we propose the cross-layer path selection decision-making module called path selection manager. Our main interest is to offer intelligent path selection decision to all applications running on ITS Station hosts, while keeping the decision process independent from any specific network layer protocol. The decision process is divided into mainly two part: the inputs of abstracted network layer parameters from SAPs to the management parameters, and the output to the network layer protocol blocks based on the decision. First, we present three management parameters required for the decision-making: ITS Station information table, path information table and application requirement list. The ITS Station information table and the path information table are newly defined following the approaches from the result of the investigation in Chapter 5, whereas the application requirement list is extended from the one that has been defined in ISO. Then we introduce how the path is selected based on these management parameters. The path selection manager are further divided into path calculation phase and the decision-making phase. In the path calculation phase, the all the candidate paths are calculated based on the information about Communication Interface (CI), Topological Locator, Nexthop, Anchor, and Capabilities. Also in this phase, the availability of the paths are estimated based on various information. As an example, we present a geographical information based path availability estimation. The results of the candidate path calculation and the path availability estimation are stored in the path information table. In the decision-making phase, the Multiple Attribute Decision Making (MADM) method is employed in the path selection algorithm. The decisions are transmitted to the network layer.

6.1 Management Parameters

The decision process is divided into mainly two part as depicted in Figure 6.1: the inputs of abstracted network layer parameters from SAPs to the management parameters, and the output to the network layer protocol blocks based on the decision.

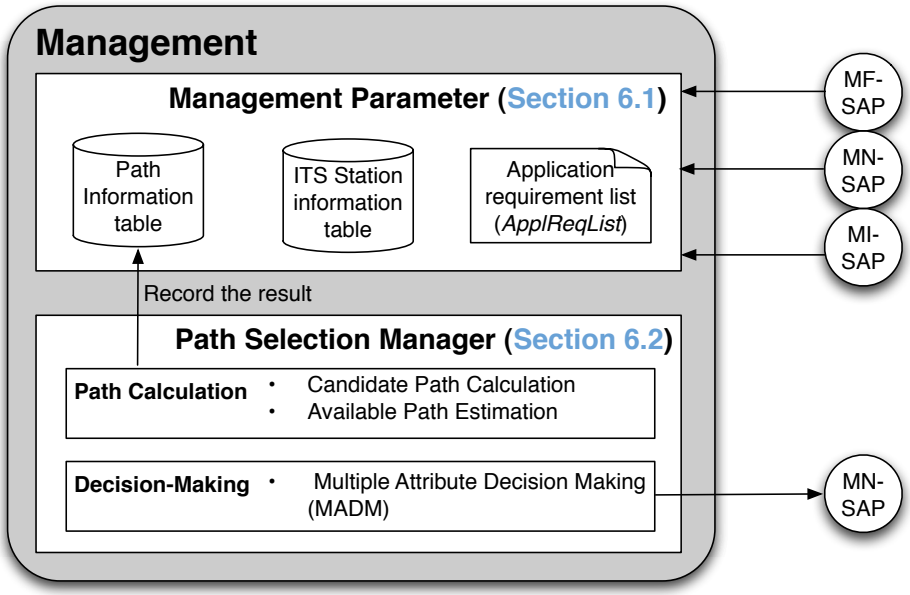


Figure 6.1: Overview of path selection manager

In this section, we shows the parameters of the ITS Station information table and the path information table. Path Selection Manager determines the path based on these tables. The parameters shown in this section are abstracted based on the conclusion of the solution design shown in Chapter 5. The mapping with actual and concrete databases in the network layer (e.g. IP and GeoNetworking) to this abstracted information is described in Section 7.3.

6.1.1 ITS Station information table

This section describes how geographic information, topological information, and service information are managed as shown in Table 6.1.

	Parameter	Description
Basic	Station ID	Identifier of ITS station. Preferably globally unique. See details in [ISO-24102-1-ITSS-management].
	Station type	Type of ITS Station. ex) Vehicle ITS-S , Roadside ITS-S
	Vehicle type	Type of vehicle. ex) car, bus, taxi, motor cycle
Topological	Locator	Topological locator of the ITS-S in the network. In the Internet, it is the network part (first 64bits) of an IP address that indicates the topological location of the node.
Geographic	Latitude	WGS-84 latitude of the ITS Station expressed in 1/10 micro degree.
	Longitude	WGS-84 longitude of the ITS Station expressed in 1/10 micro degree.
	Altitude	Altitude of the ITS Station expressed in signed units of 1 meter.
	Speed	Speed of the ITS Station expressed in signed units of 0.01 meter per second.
	Heading	Heading of the ITS Station expressed in unsigned units of 0.1 degrees from North.
	Accuracy	Accuracy indicator of the geographical position of the ITS Station
	Time stamp	The time stamp that the geographic position is recorded.
	Distance	Distance between the ITS-S and own ITS-S . The parameter is calculated from position of both ITS-S using *Haversine* formula.
	Estimated Connection	Estimated connection time in second calculated from ITS-Ss position, heading and speed.
Service		The services that the ITS-S can provide to self ITS-S . ex) DNS, DHCP, Locator Registration, Gateway and Multicast Listener.

Table 6.1: ITS Station information table

The three types of information about neighbor ITS Station are linked to an identifier of the ITS Station. In the ITS Station architecture, Station ID is defined as a globally unique identifier of ITS Station [ISO-24102-CALM-Management]. Thus the entries in the ITS Station information table can be distinguished by the Station ID. As basic information, station type (*i.e.* Vehicle ITS Station, Roadside ITS Station) is useful information to predict the movement of the station. Vehicle type is defined in [ETSI-TR-102-863-LDM] as Highly dynamic information (Type 4).

First one is the **topological information** for routing. Managing the mapping between

the identifier of an ITS Station and its topological location in the network (locator) is very important for the routing. Topological Locator indicates the location of the node in the topology of the network. A packet can be delivered by checking the topological locator as destination.

Second, the management entity needs to manage the **geographic information** of neighbor ITS Stations, as the geographic factors are often important for routing performance. The geographic information includes geographical position (latitude, longitude and altitude) and movement information (speed and direction). Some network layer protocol blocks use the geographic information directly, like GeoNetworking. In addition to the basic geographic information, the SME can obtain more detailed vehicle status information of the vehicle from the facilities layer, using LDM [ETSI-TR-102-863-LDM], CAM [ETSI-TS-102-637-2-CAM] and DENM [ETSI-TS-102-637-3-DENM] (See Section 2.2 for details). Also the SME can calculate relative information like distance to the surrounding ITS Stations with its own geographic information obtained from GPS.

The third category is the **service information**. In the network, a service is often provided by neighbor ITS Stations. Thus it is logical to manage the service information corresponding to an ITS Station information entry. The service includes locator registration, multicast, address assignment and access. There are various services not limited to the above list, and multiple service can be provided by same ITS Station.

6.1.2 Path information table

This section describes how the three types of information in the path information (CI information, path status and path metric) are managed in order to determine candidate paths. The list of the parameters is shown in Table 6.2.

The definition of a path is a set of adjoining links from a starting point to an end point. The paths are differentiated by the starting point, the end point and the intermediate points. The starting point of the path is a topological locator assigned to a CI of the ITS Station and the end point is a locator of the destination. However, the ITS Station cannot manage all the intermediate points. Typically, the furthest controllable points by the ITS Station can be an anchor (for mobility support, see details in Section 3.4.4) and the rest of the path beyond the anchor is managed by the Internet routing. Thus the path from the ITS Station can be considered equal to the path from the locator of the CI to that anchor. The ITS Station also does not manage all the intermediate portions on the path, but only the significant portions (*e.g.* MR-AR). These significant portions are recorded in the parameters category of "path status".

	Parameter	Description
CI	Link ID	Unique identifier of a VCI/CI where the path starts from. See [ISO-24102-2-Management-SAP] for details.
	Media type	The kind of a wireless communication interface is used. *CIclass*(15)
	Data rate	Data rate in the link in units of 100 bit/s (*DataRate*(5)). And *DataRateNW*(6), *DataRatesNW*(7) and *DataRateNWreq*(8)
	Cost	Price information. Cost of communication in terms of money: per byte/per second/flat-rate/free of charge. (Cost (17))
	Reliability	Percentage value indicating estimate of reliability. (Reliability (18))
	Security	Security mechanism used in wireless interface. ex) WEP, WPA
	Power Consumption	Power consumption of the interface when the interface is transmitting data and when the interface is receiving data.
	Status	Status of CI (CIstatus(42)). *e.g.* 0: not existent 1: existent 4: registered 8: active 16: connected 64: suspended 128: inactive
Path Status	Path ID	Unique Identifier to identify the path
	Locator	Identifier indicates the topological location of the ITS Station in the network.
	Next hop	ITS Station on the path that acts as a border router when packet goes beyond the network managed by a local routing protocol.
	Anchor	ITS Station that provides Locator registration function to the ITS Station .
	Reachability	Topological distance indicator from the CI. ▷on-link, ▷Local Network, ▷Extended Local, ▷ITS domain, ▷ Global Network, ▷TBD
	Capabilities	Communication capability of the path. ▷Reverse reachability for host ▷Session continuity for network ▷Session continuity for host ▷1-to-n for group ▷QoS ▷Reverse reachability for network ▷1-to-n for GeoArea ▷TBD
	Status	Status of the path. 0: not available 2: ready to be used 4: going to up 1: being used 3: potentially ready 5: going to down
	Start time	The time where the path become available. History record or estimation depending on status.
	End time	The time where the path become not available. History record or estimation depending on status.
Metric	Payload size	Size of payload for a packet using the path.
	Delay	A trip time that the wireless interface has, and actual round trip time to reach to the node in the destination scope
	Hop	Number of hops to reach to the destination.

Table 6.2: Path Information table

The first category is the **CI information**. Information about access technologies is notified from the access layer to the management entity via the MI-SAP (See Section 2.2 for details of CI and VCI). 52 CI parameters are specified in [ISO-21218:2008-CALM-Medium-SAP] as shown in Table 6.3. "I-Parame.No" indicates the identifier of the parameters. It is given as a parameters of the MI-SET and MI-GET command to respectively read and

write these parameters. The SME can access these parameters at arbitrary time using *MI-GET*, however some parameters are mandatory to be maintained in the management entity, which is called VCI performance parameter list (*VCIperformList*) (See details in [ISO-24102-1-ITSS-management], bold characters in Table 6.3). These are the actual values of performance parameters' values of VCIs and the information is kept about all the VCIs in the management entity.

AuxiliaryChannel, ControlChannel, ServiceChannel, RXsensitivity, TXpower, DataRate, **DataRateNW**, **DataRatesNW**, DataRateNWreq, **Directivity**, BlockLength, **MinimumUserPriority**, TimeOfLastReception, InactivityTimeLimit, DistancePeer, CIclass, **CommRangeRef**, **Cost**, **Reliability**, Properties, CommProfile, MinimumSuspendPriority, Medium, NWsupport, CIaccessClass, RegulatoryInformation, FreeAirTime, SIMpin, ProviderInfo, MediumUsage, MedUseObservationTime, SuspendSupportFlag, QueueAlarmThreshold, QueueLevel, MACaddress, MACaddrTemp, TimeoutRegister, MedID, VirtualCI, FrameLengthMax, KinematicVectorIn, KinematicVectorOut, CIstatus, Notify, MinPrioCrossCI, CckId, PeerMAC, QueueLowThreshold, PeerRXpower, TXpowMax, ManufacturerDeviceID, Connect

Table 6.3: 52 CI parameters specified in [ISO-21218:2008-CALM-Medium-SAP]

VCIperformList is also useful to see the path performance. Beside *VCIperformList*, we list important parameters from access technologies in Table 6.2 ((Number) after CI parameter name indicates *M-Param.No* in the Table). Media type, data rate, cost and reliability are CI parameters via the MI-SAP. These are important parameters to determine the path.

The second category is **path status** that includes the information about the parameters that characterize the path including the ITS Station information that is in the middle of the path (AR, HA, MR and CN), capability of mobility support, topological locator of the starting point, availability of the path, reachability of the path and etc. Path status is provided by network parameters that come from MN-SAP. Some paths can be created from same CI using different routing protocols, different next hops and anchors. These paths are identified by path ID. Topological locator indicates the topological location of the node and the access network where the CI is attached to.

The "reachability" field indicates which part of the network is reachable beyond the neighbor ITS Station. In principle, just after configuration of a VCI, the VCI cannot reach beyond anywhere before the network layer configurations, except for On-link. As network configuration progresses, the path completed reachability extended to reach more nodes beyond On-link. The state is stored in the reachability field as On-link, Local Network, Extended Local, ITS domain and Global Network (Note that the difference is depicted in Figure 6.2).

On-link Reachability to ITS Stations that are one hop away from the source ITS Station. Typically, it corresponds to ITS Stations within the radio range of a wireless interface. In the range, the source ITS Station can reach them without any routing protocol.

Local Network Reachability to the ITS Stations that are in the network controlled by a local routing protocol. In vehicle ITS Station case, it is the reachability to the vehicle and roadside ITS Stations in a wireless multi-hop vehicular ad-hoc network. Some routing protocols enable multi-hop communication.

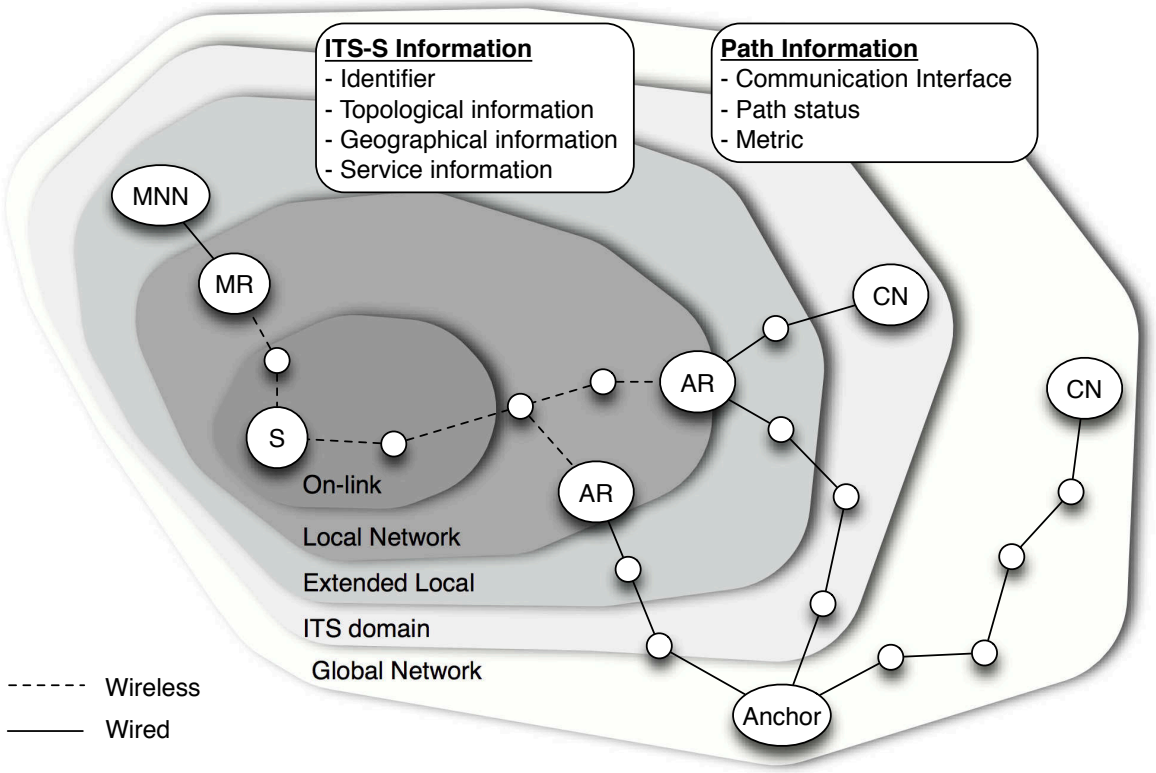


Figure 6.2: Network around vehicle ITS station

Extended Local Reachability to the ITS Station internal nodes of the neighbor ITS Stations in the Local Network. Typically, the ITS Station internal nodes attached behind an ITS Station router in a vehicle or an ITS Station router in roadside ITS Station do not have a routing function. A protocol is needed to exchange the station internal prefix in order to reach nodes attached to the neighbor ITS Station.

ITS domain Reachability to central ITS stations that provide ITS services. Depending on the security policy or administration policy, ITS domain may not provide the reachability to the Global Network.

Global Network Reachability to all the other nodes in the connected network. To enable global reachability with moving environment, session continuity capability may be required.

Note that the reachability may not be established in the above order (on-link→Local Network→Extended Local→ITS domain→Global Network). Some CI may acquire Global Network reachability just after On-link reachability without accessing Local Network (e.g. 3G, WIMAX).

The management entity maintains also "status" in the path information table. The management entity stores the information of all the paths that includes:

***Available path*:** Path that is established and ready-to-use.

***Candidate path*:** Path that is theoretically possible but not ready-to-use. *Candidate paths* are calculated in the management entity from the combination of the entries contained

in ITS Station information table (See Section 6.2.1).

"Status" of the paths shows the availability of the path. Status can be either "being used", "ready to be used", "potentially ready", "going up", "going down", or "not available" as shown below. The lifetime of the path is maintained as the estimated starting time and ending time of the availability. The lifetime is linked with the status field.

"being used" The path is used. When the path is in this status, the starting time is the history records when the path became available and the ending time is the estimated time of unavailability.

"ready to be used" The path is ready to be used. When the path is in this status, the starting time is the history records when the path became available and the ending time is the estimated time of unavailability.

"potentially ready" The path potentially exists but it is not managed yet. *i.e.* Path selection manager is aware of the possibility of the path, however it is not sure the path could become available before a trial is performed. When the path is in this status, both the starting time and the ending time are left empty.

"going up" The path is going to be available. When the path is this status, the starting time is the estimated time of availability and the ending time is the estimated time of unavailability.

"going down", The path is going to be unavailable. When the path is in this status, the starting time is the history records when the path became available and the ending time is the estimated time of unavailability.

"not available". The path is unavailable. When the path is in this status, both the starting time and the ending time are the history records of the last available time.

In all cases, if the estimation is not possible, the estimated time is left as empty. See an example of the estimation in Section 6.2.2.

The third category is **path metric** that is determined by the network layer protocol or the lower layers. Examples of path metrics are propagation delay, payload size, and number of hops. To obtain the propagation delay, same measurement is needed. The payload size is often determined by the underlying technologies. For example, since wireless interfaces have specific MTU and the network layer protocol blocks have specific size of header encapsulation, the payload size of the path can be often calculated. The number of hops is obtained by measurement, or provided by some routing protocol.

We leave room to add other parameters in the path information table for future extension.

6.1.3 Flow requirement table

The path selection manager selects a path that satisfies the *application requirements*. The application requirements are maintained in the management entity as a management parameter as specified in [ISO-24102-1-ITSS-management]. The parameters are notified to the SME using MF-REQUEST "*ITS-S-Appl-Reg*" as in [ISO-24102-CALM-Management]. Currently in ISO, following four parameters are specified as *ApplReqList*: Data rate, Cost, Network protocol support and Type of CI.

Although formats of *ApplReqList* and *ITS-S-Appl-Reg* are specified as in Appendix C, both formats have room for future extension. We propose the flow requirement table in order to accommodate the requirement for the delay and stability as follows:

- QoS requirements
  - **Data rate**: Minimum average data rate requested at the MI-SAP in 100 bit/s. Corresponds with I-parameter 6.
  - **Stability**: Indicator how long the path is assumed to last in order to estimate probability of packet loss due to handover.
  - **Delay**: A trip time that the wireless interface has, and actual round trip time to reach to the node in the destination scope in milli second.
- Operational requirements
  - **Monetary cost**: Maximum acceptable cost of the link-usage in terms of money. Corresponds with I-parameter 17.
- Security requirements
  - **Network layer Security**: L3 layer security required.
  - **Wireless security**: L2 layer security required.
- Data plane module
  - **Network protocol block**: Network protocol required.
  - **Type of CI**: Type of CI required.

With such additional parameters, the path selection manager can be aware about which application is sensitive to which parameters of data rate, monetary cost, delay and stability.

6.2 Path Selection Manager

Figure 6.3 shows the flow chart of the path selection manager. It starts from preparation of decision-making that are:

- Candidate path calculation described in Section 6.2.1 and
- Path availability estimation described in Section 6.2.2

Then in decision phase, there are two modes of decision:

- Best available path determination searches for the path that satisfy the application request in the flow requirement table in all available paths (Section 6.2.3)
- Best candidate path determination searches for the path that satisfy the application request in the flow requirement table in all candidate paths (Section 6.2.4)

The resulting decisions are as follows:

- ***FlowPolicy*** commands the flow policy to set how to use established paths,

- ***PathMNG*** commands establishment and management of paths, and
- ***STAServDiscov*** commands searching a new path with service discovery

If the path satisfies the application requirements is found from available paths in path information table as the result of Best available path determination, the correspondent flow policy is provided to the network layer (see MN-COMMAND "FlowPolicy" in Chapter 7). If not, the Best candidate path determination searches the paths that satisfies the application requirements from the candidate paths in the path information table. If it is found, the management entity instructs the network layer to establish the path (See MN-COMMAND "PathMNG" in Chapter7), if not, it instructs the network layer to look for other paths (See MN-COMMAND "STAServDiscov" in Chapter 7).

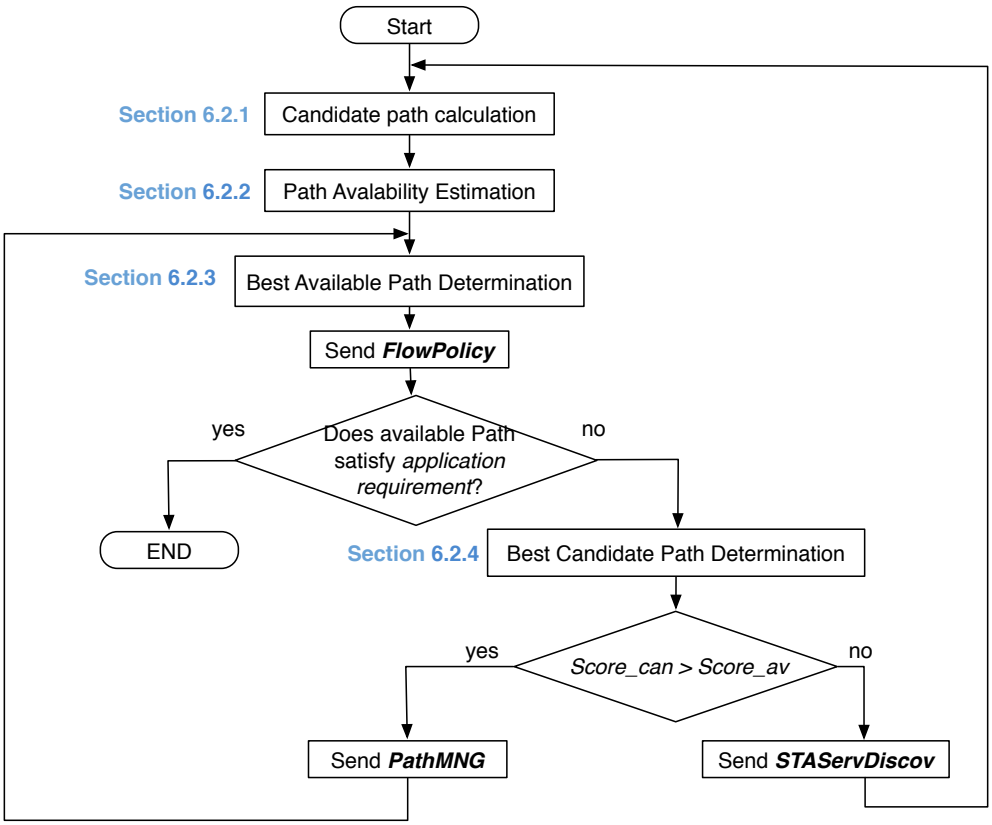


Figure 6.3: Path Selection Manager Algorithm

6.2.1 Candidate path calculation

The management entity maintains path status in the path information table. The management entity stores the information about all available paths and candidate paths as described in Section 6.1.2.

Figure 6.4 shows an example of both available paths (from (a) to (d)) and candidate paths (from (1) to (7)) between a source ITS Station to a destination ITS Station. In the example scenario, the source ITS Station has three CIs (11p, 11g, 3G) and a VANET protocol is available on the 11p interface. The source ITS Station has information about four neighbor roadside ITS Station serving as ARs connecting from both 11p and 11g interfaces in the ITS

Station table. In addition to the ARs, the ITS Station also has two anchors registered in the table. In the scenarios, the management entity has at least eleven path information entities that are illustrated in Figure 6.4 from the combination of path information table's parameters (CI, Topological Locator, Nexthop, Anchor, and Capabilities).

Actually, the set of candidate paths is not limited to the eleven paths. For example, the management entity can store more paths including optimized path or the direct path from a topological locator to the destination ITS Station without passing to the anchor. How to calculate the candidate paths is up to the algorithm in the management entity. Also how to assign unique path IDs to the paths is up to the algorithm.

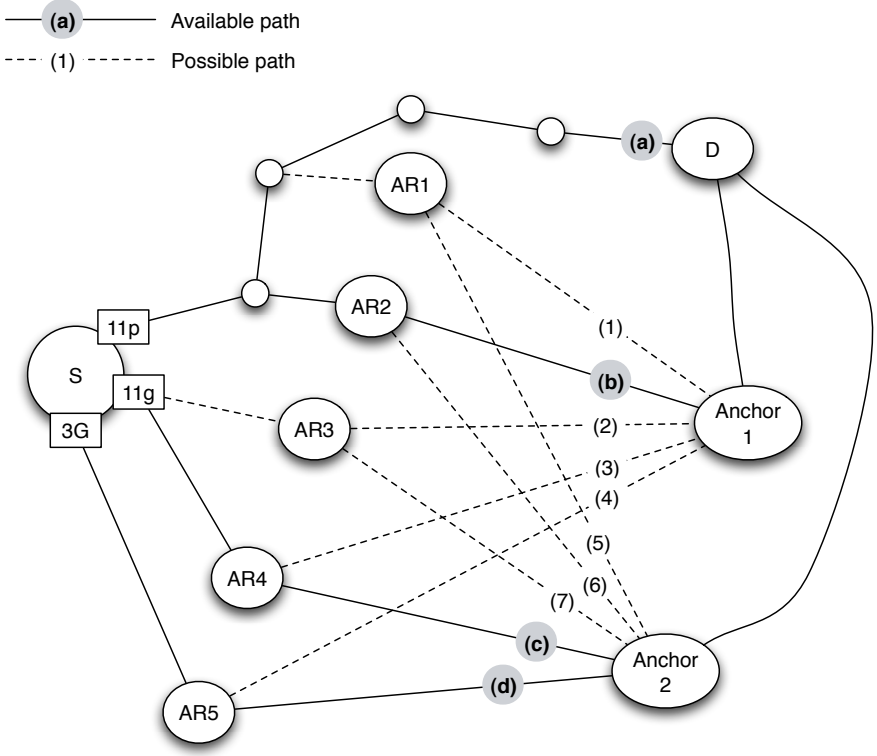


Figure 6.4: Available paths and candidate paths

In the example, there are vehicle-based path and Internet-based path between the source (S) and the destination (D). Path (a) is a direct path to the destination ITS Station from the VANET interface on 11p. The path is notified to the SME when the source ITS Station receives the direct path from the destination ITS Station. Paths (b,c,d) are Internet-based available paths. The paths are notified to the SME when the path is established. Also, it is notified when the path becomes unavailable. *e.g.* Binding is successfully registered in NEMO.

Paths (from 1 to 7) are candidate paths that are not yet established, but they can become ready-to-use after path establishment. The available path and the candidate paths are differentiated by the following information in the path information table:

- Wireless interface (11p, 11g and 3G),
- Topological Locator (CoAs),
- Nexthop (MR1, AR1, AR2, AR3, AR4 and AR5),

- Anchor (HA1 and HA2)
- Capabilities (session continuity)

6.2.2 Path Availability Estimation

The availability path estimation function estimates if the path is available or unavailable and when the path becomes available and unavailable from various information.

Path availability often depends on the connection from the self ITS Station and a neighbor ITS Station that provides "access" service. *i.e.* AR. One good way to estimate the availability of the paths is using the geographical position and movement information stored in the ITS Station information table. This section describes geographic information based path availability estimation. A more intelligent one can replace in the future if more information is available. *i.e.* Co-operative Awareness Messages (CAM), Decentralized environmental Notification Messages (DENM) and Local Dynamic Map (LDM) (See Section 2.2 for details).

To estimate when the path becomes available and unavailable, first, distance between the self ITS Station and all the neighbor ITS Stations in the ITS Station information table is calculated.

When the ITS Station's latitude and longitude are defined as $lat1$ and $long1$ and a neighbor ITS Station's latitude and longitude are defined as $lat2$ and $long2$, the distance d to the neighbor ITS Station is given the *Haversine* formula shown in equation 6.1.

$$\begin{cases} d = R \cdot acos\left[sin\left(lat1\right) \cdot sin\left(lat2\right) + cos\left(lat1\right) \cdot cos\left(lat2\right) \cdot cos\left(long2 - long1\right)\right] \\ R = 6378.7km\left(earth's\, radius\right) \end{cases} \tag{6.1}$$

The obtained distance to the neighbor ITS Station is recorded in the distance field of the ITS Station information table. Then the management entity estimates the available time of each neighbor ITS Station as follows. Figure 6.5 shows an example of path availability estimation when a path is available via an neighbor ITS Station which provides a "Next hop" service.

The management entity knows its position $(Lat1, Long1)$ and heading $\theta 1$ and also neighbor ITS Station's position $(Lat2, Long2)$. The management entity estimates the time T that the ITS Station is within radius r of a neighbor ITS Station, assuming that it moves straight with settled direction.

First, the distance d to the neighbor ITS Station is calculated by *Haversine* formula shown in equation 6.1. Then the angle of direction of the neighbor ITS Station from the ITS Station $\theta 2$ is calculated by equation 6.2, where dx is the distance between the ITS Station and the neighbor ITS Station in latitude offset.

$$\begin{cases} \theta 2 = acos(\dfrac{dx}{d}) \\ dx = R \cdot acos\left[sin\left(lat1\right) \cdot sin\left(lat2\right) + cos\left(lat1\right) \cdot cos\left(lat2\right)\right] \\ R = 6378.7km\left(earth's\, radius\right) \end{cases} \tag{6.2}$$

When the ITS Station moves straight, the nearest distance to the neighbor ITS Station will be distance n as in figure 6.5. The distance n is given by equation 6.3, where $\theta 1$ is the heading of the ITS Station.

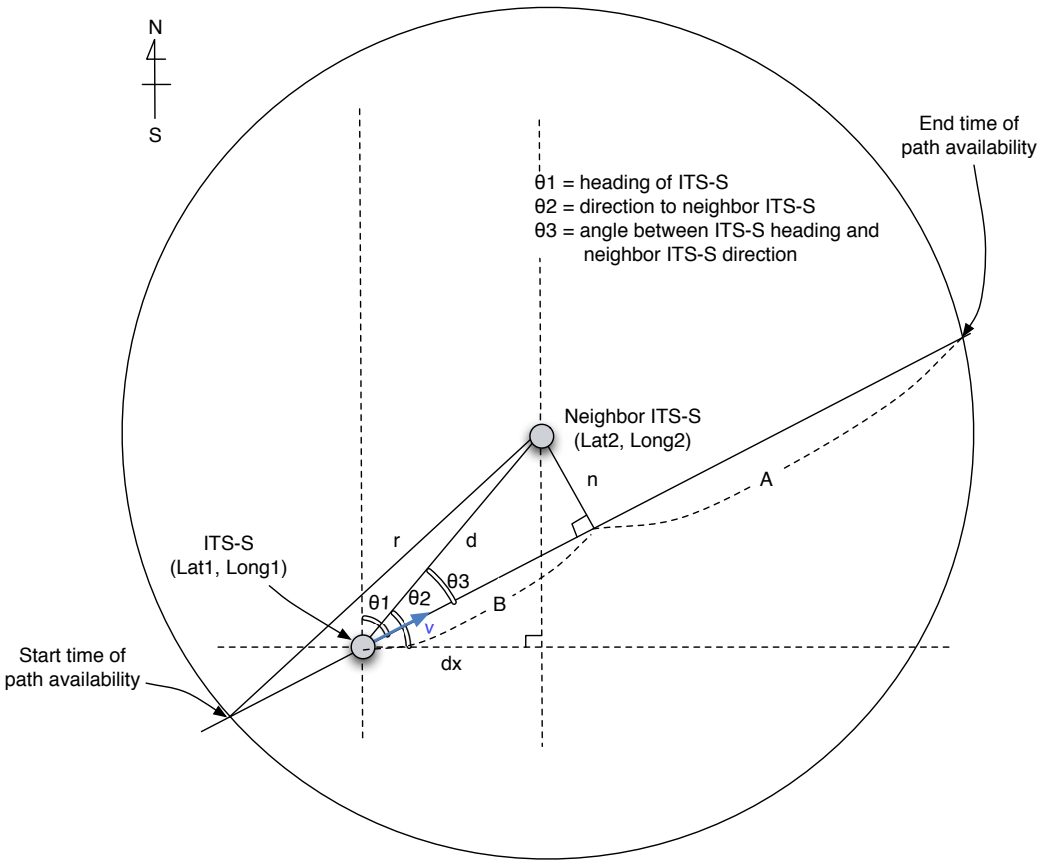


Figure 6.5: Path Availability Estimation

$$\begin{aligned} n &= d \cdot sin(\theta 1 + \theta 2 - 90) \\ &= d \cdot [sin(\theta 1 + \theta 2) \cdot cos(90) - cos(\theta 1 + \theta 2) \cdot sin(90)] \\ &= d \cdot [-cos\,(\theta 1 + \theta 2)] \end{aligned} \tag{6.3}$$

Once the current distance to the neighbor ITS Station, the nearest distance to the neighbor ITS Station and radius of the neighbor ITS Station are given by d, n and r, respectively, we can calculate the estimated distance the ITS Station will be in the radius r of the neighbor ITS Station. The distance A that is between the point of entry to the neighbor ITS Station's radius r and the nearest point to the neighbor ITS Station in the ITS Station's way is calculated by the *Pythagorean* theorem as well as the distance B where the ITS Station reached the nearest point to the neighbor ITS Station. That is equation 6.4.

$$\begin{aligned} A &= \sqrt{r^2 - n^2} \\ B &= \sqrt{d^2 - n^2} \end{aligned} \tag{6.4}$$

Thus the estimated time T during which the ITS Station is in the radius r of the neighbor ITS Station is given by equation 6.5, where v is the velocity of the ITS Station.

$$\begin{cases} T = \dfrac{A+B}{v} & (When\ MR\ is\ approaching\ to\ AR) \\ T = \dfrac{A-B}{v} & (When\ MR\ is\ leaving\ from\ AR) \end{cases} \tag{6.5}$$

The estimated available time of the neighbor ITS Station obtained from the above equation depends on the assumption that the ITS Station moves straight with the heading of the self ITS Station at the moment. The assumption keeps the decision mechanism simple, however it would be preferable to have more accurate estimated time with the support of movement prediction. For example, digital maps, car navigation system, mobility model and statistical analysis of itinerary history and etc.

The obtained estimation about when the path becomes available or unavailable is stored as "start time" and "end time" fields in the path information table.

6.2.3 Best available path determination

Best available path determination searches the most suitable path in the available path table. If it finds the path that satisfies the application requirements in the flow requirement table, it sets the flow policy for the flow from the application to the path using MN-COMMAND "*FlowPolicy*". If not, it selects the most appropriate path from the available path anyway and is set the flow policy to the best path (See Figure 6.3).

Best available path determination takes the following application requirements parameters as minimum requirements (the other application requirements can be used optionally):

- Data rate,
- Monetary cost,
- Delay and,
- Stability

Best available path determination matches the above parameters with the path information table. Table 6.4 shows a snapshot of path information table that corresponds to the scenario illustrated in Figure 6.4 in Section 6.2.1. The path ID (AP_1..., AP_4) indicates available path and Path ID (CP_1,CP_2...) indicates candidate path.

If a path that satisfies all the application requirements is found from the available path list (AP_1..., AP_4) , the path is selected. If there are multiple available paths that satisfy the application requirements, it should select the best one. If no path satisfies the application requirements it should find the best available paths.

The best available path can be selected by the MADM Methods [Rao2007]. In the MADM methods, a decision matrix has four main parts : (i) alternatives, (ii) attributes, (iii) weight or relative importance of each attribute, and (iv) performance measure of alternatives with respect to the attributes. In the best available path determination as in Table 6.4, the main parts of MADM are translated as follows:

- Alternatives → Available Paths AP_i (for $i = 1, 2, 3, ..., N$) and Candidate Path CP_j (for $j = 1, 2, 3, ..., M$)

[1] MBytes/euros, depending on the country, day and time

ID	CI			Path status					Path metric		
Attribute	A_1 media	A_2 cost[1]	A_3 data rate	A_4 Next	A_5 Anchor	A_6 Status	A_7 Start	A_8 End	A_9 Payload	A_{10} delay	...
weight	w_1	w_2	w_3	w_4	w_5	w_6	w_7	w_8	w_9	w_{10}	...
AP_1	11p	0	15 Mbps	MR	—	2	-30 s	20 s	1420 B	10 ms	...
AP_2	11p	0	10 Mbps	AR2	HA1	2	-40 s	50 s	1380 B	30 ms	...
AP_3	11g	0	20 Mbps	AR4	HA2	2	-50 s	10 s	1460 B	30 ms	...
AP_4	3G	1	0.5 Mbps	AR5	HA2	2	-1000 s	—	1460 B	200 ms	...
CP_1	11p	0	15 Mbps	AR1	HA1	3	+2 s	50 s	1380 B	—	...
CP_2	11g	0	10 Mbps	AR3	HA1	3	+2 s	20 s	1460 B	—	...
CP_3	11g	0	10 Mbps	AR4	HA1	3	+2 s	10 s	1460 B	—	...
CP_4	3G	1	0.5 Mbps	AR5	HA1	3	+3 s	—	1460 B	—	...
...	...	...	...	...	...	...	...	...	...	...	...

Table 6.4: Example of path information table

- Attributes → Attributes A_l (for $l = 1, 2, 3, ...L$), ex. (A_1 =media, A_2 =cost, A_3 =data rate, ...)
- Weight → Weight w_l (for $l = 1, 2, 3, ...L$)
- Measure → Measure m_{il} (for $i = 1, 2, 3, ..., N; l = 1, 2, 3, ..., L$) for Available Path, and m_{jl} (for $j = 1, 2, 3, ..., M; l = 1, 2, 3, ..., L$) for Candidate Path

Among MADM methods, we use the simplest method named Simple Additive Weighing (SAW) Method [Fishburn1967]. In SAW, each weight is given to each attribute and the sum of given weight w_l (for $l = 1, 2, 3, ...L$) must be 1. Each path is evaluated with regard to every attribute and each given weight. When the attributes are not expressed in identical units of measure (*e.g.*, only seconds, only Mbps, only milliseconds, etc), the decision matrix has to be normalized. SAW can be used for any type and any number of attributes by the normalization. Normalized value of measure m_{il} is expressed by Equation 6.6.

$$\begin{cases} (m_{il})_{normalized} = \dfrac{(m_{il})_K}{(m_{il})_{max}} & (When\ the\ attribute\ is\ beneficial) \\ (m_{il})_{normalized} = \dfrac{(m_{il})_{max}}{(m_{il})_K} & (When\ the\ attribute\ is\ non-beneficial) \end{cases} \tag{6.6}$$

where $(m_{il})_{normalized}$ is the normalized value of measure m_{il}, $(m_{il})_k$ is the measure of the attribute for K-th path, and $(m_{il})_{max}$ is the measure of the attribute for the max-th path that has the highest measure of the attribute out of all paths considered. The higher measure is favorable in beneficial attributes (*e.g.*, A_3 =data rate, A_8 =end time, and A_9 =payload, etc) and on the contrary, the lower measure is desirable in non-beneficial attributes (*e.g.*, A_2 =cost).

Some measures of the path information table are filled with the ITS Station ID that is the kay parameter in the ITS Station information table. (*e.g.* A_5 =Next and A_6 =Anchor). We can take the distance to the neighbor ITS Station into account to evaluate the quality of the path.

The numbers between 1 and 9 can be calculated for the measures that are not expressed by number (e.g., security). The measure of such attributes are equal-spaced numbers whose

space-gap SG between subsequent measure is given by Equation 6.7.

$$SG = (m_{most} - m_{least})/N_m \tag{6.7}$$

where the measure of most preferred configuration, least preferred configuration and number of measurement are given by m_{most}, m_{least} and N_m. In the security case, $m_{weak} = 1$, $m_{normal} = 5$ and $m_{strong} = 9$ can be allocated to the security configuration corresponding to *weak*, *normal* and *strong*.

The overall performance score $Score_i$ of an available path AP_i is given by Equation 6.8.

$$Score_i = \sum_{l=1}^{M} w_l \cdot (m_{il})_{normalized} \tag{6.8}$$

The overall performance scores $Score_i$ are compared for $i = 1, 2, 3...N$, then the available path that have the highest score $Score_{av}$ is selected in the best available path determination. The flow from the application is set to the selected available path using *FlowPolicy*.

If the selected available path satisfies all the application requirements, a cycle of path selection manager terminates. Otherwise, the path selection manager goes to the next step to try to determine a better path than the available path as described in the next section (See overview in Section 6.2).

6.2.4 Best Candidate path determination

When the selected available path does not satisfy the application requirements, the path selection manager searches for an appropriate path from the candidate path list. Similarly to the best available path determination described in Section 6.2.3, the best candidate path determination can be solved with SAW. The overall performance score $Score_j$ of a candidate path CP_j is given by Equation 6.9.

$$Score_j = \sum_{l=1}^{M} w_l \cdot (m_{jl})_{normalized} \tag{6.9}$$

where $(m_{jl})_{normalized}$ is the normalized value of measure m_{jl}.

The overall performance scores $Score_i$ are compared for $j = 1, 2, 3...M$, then the candidate path that has the highest score $Score_{can}$ is selected as the best candidate path.

If the selected candidate path has a better score than the selected available path in Section 6.2.3 ($Score_{can} > Score_{av}$), the candidate path is more favorable than the currently used path. Thus the SME sends *PathMNG* to the network layer in order to establish the candidate path with the specified CI, topological locator, next-hop, and anchor. Then, the cycle of the path selection manager goes to the best path determination described in Section 6.2.3. If the specified path is successfully established, the established path can be selected for the best available path at the next time in the cycle.

If the selected candidate path has a lower score than the selected available path in Section 6.2.3 ($Score_{can} < Score_{av}$), all the candidate paths are less favorable than the currently used path. The selected available path does not satisfy the application requirements. Thus the SME sends "*ServDiscov*" to the network layer in order to increase the candidate paths.

Chapter 7

Cross-layer Path Selection Parameters and Primitives

Contents

In this chapter, we present the cross-layer primitives and parameters for path selection. Four primitives are required for the interaction between the SME and the SNT. First, we propose two new primitives (*MN-GET* and *MN-SET*) allowing the path selection manager to access to some of the parameters (*N-Parameter*s) recorded in the existing Management Information Base (MIB) of the IPv6 and TCP/UDP protocol blocks in the SNT. The two other ones (*MN-REQUEST* and *MN-COMMAND*) are needed to instruct the IPv6 protocol block to route flows to a given path and correspond to the primitives already defined in ISO specifications for a network layer protocol block other than IPv6 (i.e. FAST). We thus extend these primitives to transfer the necessary information between the path selection manager and the IPv6, GeoNetworking and TCP/UDP protocol blocks of the SNT. We figure out that the current ISO specification of *MN-REQUEST* and *MN-COMMAND* commands do not fulfill our design requirements described in Chapter 4. Thus we define five new *MN-REQUEST* commands (*STAGeoNot*, *STATopoNot*, *STAServNot*, *PathNot*, and *PathMetricNot*) and three new *MN-COMMAND* commands (*STAServDiscov*, *PathMNG*, *FlowPolicy*) to accommodate our needs for path selection.

Then we explain how these commands are actually used. To do so, we first present the mapping between the abstracted parameters contained in the ITS station information, Path information and Flow requirement tables in the ITS station management entity and the corresponding parameters in the IPv6 and GeoNetworking protocol blocks of the ITS station network & transport layer. Then, to show the interaction between the management entity and the network layer, we describe the complete path selection procedure, from the activation of Communication Interfaces (CIs) to the transmission of flow policy instructions.

Note that this study is based on year 2011 versions of the ISO Standards and that the standards constantly evolve. As a result, primitives and parameters of the MN-SAP may have changed at the time of reading.

7.1 N-Parameter Based Message Exchange

The MN-SAP is illustrated on Figure7.1. First, the N-Parameter based parameters exchange (*MN-SET* and *MN-GET*) is presented in Section 7.1. Then, the parameters and primitives for path selection *(MN-REQUEST* and *MN-COMMAND*) are presented in Section 7.2.

7.1.1 N-Parameter

As well as I-Parameter is specified in [ISO-24102-2-Management-SAP] for the access layer, we define N-Parameter in the network layer is a set of virtual databases. The modules in the network layer update N-Parameter according to network status change. Also, N-Parameter defines default behavior of the network module. *MN-GET* and *MN-SET* explained in Section 7.1.3 provide for SME the ways to read and write the values of N-Parameter.

In IPv6, some of the necessary network protocol blocks already have a virtual database called MIB defined in IETF. Objects in the MIB are defined using a subset of Abstract Syntax Notation One (ASN.1) [ITU-T-X.680-ASN1:2002] called Structure of Management Information Version 2 (SMIv2) [rfc2578]. MIB is often used in Simple Network Management Protocol (SNMP)[rfc3411], the term is also used more generically in contexts such as in OSI network management model.

The MIB for TCP is specified in [rfc4022] and for UDP is specified in [rfc4113] in the transport layer. In the IP layer, MIBs for IP [rfc4293], for IP tunnel[rfc4087], for Mobile

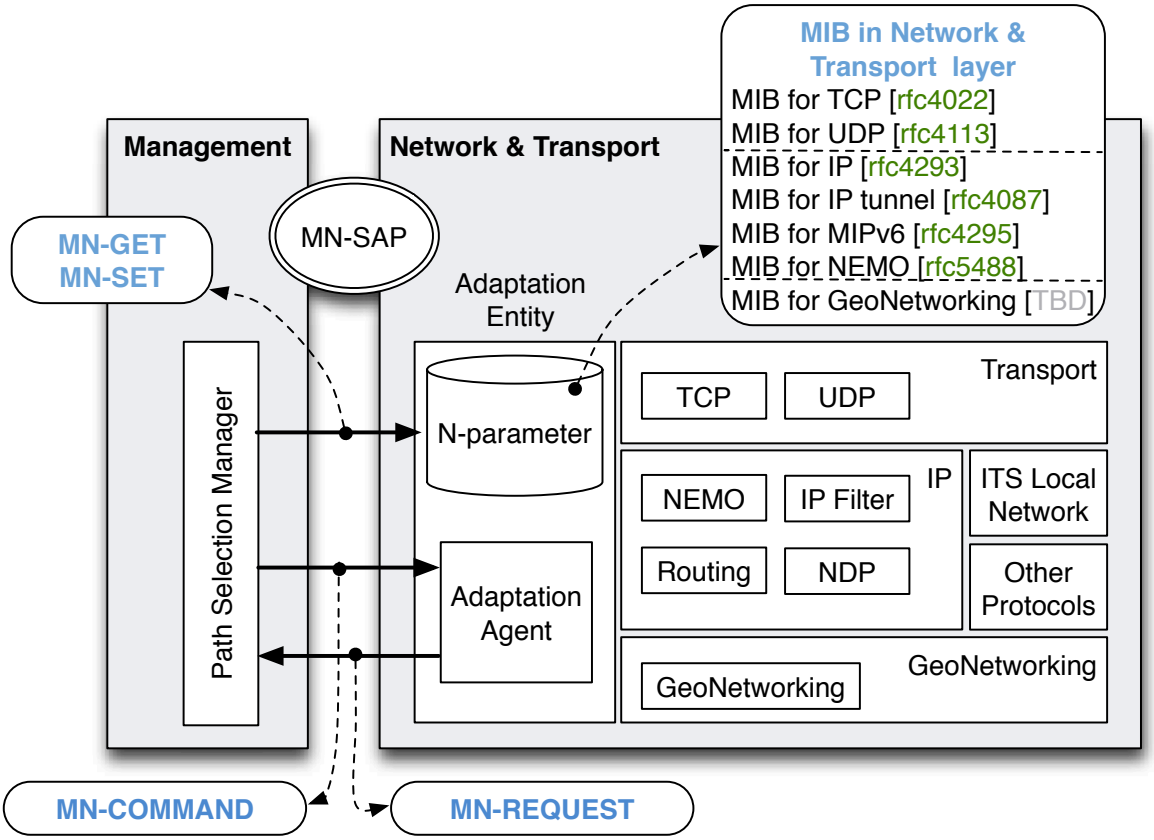


Figure 7.1: Interface Between the Management Entity and the Network Layer

IPv6 [rfc4295] and for NEMO [rfc5488] have been defined by the IETF, as well. On the other hand, the MIB for GeoNetworking is not defined yet in any organization. Thus we listed the necessary object in Section 7.1.2.

Note that MIB is also going to be defined in the management entity as found in the ITS Station architecture (see details in Section 2.2.1), however the MIB in the management entity is not the same database as N-Parameter and out of focus in this study. The roles of N-Parameters in the network and the MIB in the management entity should not be duplicated. The N-Parameters in the network layer are considered as the parameters that define the default behavior of the network and transport layer. On the other hand, the MIB in the management entity is considered as database stored in order to respond the request of read/write to the parameters (*i.e.* SNMP). When there are common parameters in the management entity and the network layer, a value of an object of MIB in the management entity are symbolic links to the correspondent N-Parameter in the network layer. When SME is requested to read/write to such parameters, it redirects the request to the N-Parameter using *MN-GET* and *MN-SET* (defined in Section 7.1.3) via MN-SAP.

7.1.2 N-Parameters for GeoNetworking

We classify the parameters into the basic setting of GeoNetworking and five main functions such as Communication Interface (CI), Location Table (LT), Beaconing, Location Service (LS) and Forwarding. Table 7.2 shows all the parameters for GeoNetworking. We keep the statistics table for GeoNetworking for future work (Such statistics for IP are defined in MIB

for IP as IP statistics table in [rfc4293]). All the parameters should be accessible from the management entity by $MN-GET$ and $MN-SET$ with read and write permission.

	Parameter	Description
Basic	*GeoCapability*	This object indicates whether the GeoNetworking function is enabled.
	GeoNodeID	This object indicates *GN_ADDR* in [ETSI-TS-102-636-4-1-Media] that could be updated for privacy reasons (*i.e.* pseudonym).
CI	*GeoIpInterfaceIndex*	The index to uniquely identify the interface between GeoNetworking and IP.
	GeoAccess InterfaceIndex	The index to uniquely identify the interface between GeoNetworking and Access. ex. egress interface.
LT	*LocationTableLifeTime*	This object indicates the default lifetime of the entry in the location table.
	LocationTableMaxNode	This object indicates the maximum number of the nodes storing in the location table.
	LocationTableEntry	This object indicates the entries of location table.
Beacon	*BeaconInterval*	This object indicates the default time interval of beacons.
	BeaconHopLimit	This object indicates the default hop limit of beacons.
LS	*LocationServiceType*	The object indicates the default type of Location Service (ex. flooding, request-reply, etc.)
	LocationService HopLimit	This object indicates default hop limit of location service message.
	LocationService RetransTimer	The objects indicates the default time interval to resend the request of Location Service.
Forwarding	*StoreForwardLifeTime*	The object indicates the lifetime of storing packets, when the node is out of destination area.
	StoreForwardMaxSize	This object indicates the maximum size of packet stored in the node for store and forward.
	TrafficHopLimit	This object indicates default hop limit of traffic packet.
Others	*PositionVector*	The object indicates the position vector of the ITS-S.
	GeoDestination	The object indicates the mapping between group ID and geographic destination area.

Figure 7.2: N-Parameters for GeoNetworking

GeoCapability and *GeoNodeID* are defined as basic setting. The management entity determines whether the GeoNetworking function is enabled or not using *GeoEnableStatus*. Also, it can enable and disable the GeoNetworking function using *GeoEnableStatus*. *GeoNodeID* indicates the GeoNetworking ID (*GN_ADDR* in [ETSI-TS-102-636-4-1-Media]) used in the ITS Station. For preventing the location privacy issue, the management entity may change the GeoNetworking ID in certain interval so that the node uses the ID as a pseudonym. *GeoNodeID* provides a means to change the GeoNetworking ID via *MIBset*.

GeoAccessInterfaceIndex and *GeoIpInterfaceIndex* are defined as CI parameters. *GeoAccessInterfaceIndex* indicates the index of the egress interface of GeoNetworking and

$GeoIpInterfaceIndex$ indicates the index of virtual interface between GeoNetworking and IP. The former object is mandatory for all the GeoNetworking nodes because all of them have the egress interface. On the other hand, later object is used only in IPv6 GeoNetworking, when GeoNetworking gives the packet to the IP layer or vice versa. These objects only provides the interface index, however the management entity can find corresponding locator and identifier (*i.e.* IP address or prefix information) of the ITS Station by the interface index using MIB for IP.

$LocationTableLifeTime$, $LocationTableMaxNode$ and $LocationTableEntry$ are defined as LT parameters. $LocationTableLifeTime$ indicates the default lifetime of the Location Table entries. When neighbor nodes are moving fast and are organizing very dynamic network topologies, a neighbor ITS Station position kept as a Location Table entry cannot be fresh for long time. Thus the lifetime of Location Table should be configured shorter. $LocationTableMaxNode$ indicates the maximum number of nodes stored in the Location Table. In a traffic jam situation, many neighbor ITS Station position stored in the Location Table amplifies the calculation time of the next hop GeoNetworking node. The management entity can set proper number of nodes in Location Table to avoid performance degradation. $LocationTableEntry$ indicates the entries of Location Table. The management entity get the position information of neighbor GeoNetworking nodes including GeoNetworking ID, latitude, longitude, altitude, speed, heading and lifetime.

$BeaconInterval$ and $BeaconHopLimit$ are defined as beacon parameters. $BeaconInterval$ indicates the time interval between beacons. In the GeoNetworking layer, the position of the ITS Station should be updated frequently because the Location Table entry in the neighbor node cannot be fresh. On the other hand, in case of traffic jam, the frequent updates of the Location Table entries are not necessary, in contrary, the frequent beacons from many GeoNetworking node cause congestion of traffic. Thus in low-speed situation, longer time interval between beacons is favorable. $BeaconHopLimit$ indicates the hop limit of the beacons. Normally, the hop limit is set as 1, however multi-hop beaconing is considered as an advanced feature of GeoNetworking. Multi-hop beaconing allows a GeoNetworking node to get the position of neighbors several hops away. In packet transmission, the node can avoid to send Location Service request when it has the position of the destination node in Location Table. Thus multi-hop may improve the delay by increasing the possibility to avoid Location Service signaling. There is a trade-off between the delay and network traffic congestion because of beacon flooding.

$LocationServiceType$, $LocationServiceHopLimit$ and $LocationServiceRetransTimer$ are defined as Location Service parameters. $LocationServiceType$ indicates the default Location Service type including the flooding and request-reply signaling. The management entity can decide how to get the destination position depending of the situation. $LocationServiceHopLimit$ indicates the default hop limit of Location Service. Normally, the value is set as 255. $LocationServiceRetransTimer$ indicates the default time interval of resending Location Service request when the node has no Location Service reply.

$StoreForwardingLifeTime$, $StoreForwardingMaxSize$ and $TrafficHopLimit$ are defined as forwarding parameters, . $StoreForwardingLifeTime$ indicates the lifetime of stored packets when the destination node is not its neighbor. The stored packets can be delivered to a longer distance with longer lifetime of storing packets. Thus it increases possibility to reach the destination, however there are a trade-off between memory for storing packets and calculation time in the forwarding table. $StoreForwardingMaxSize$ indicates the maximum total size of stored packets. $TrafficHopLimit$ indicates the default hop limit of traffic packet.

PositionVector and *GeoDestination* are defined as the other parameters. *PositionVector* indicates the position vector of the nodes including latitude, longitude, altitude, speed, heading and lifetime. *GeoDestination* indicates the mapping between multicast address and the geographical destination area (GeoDestination) defined in [ETSI-EN-302-931-GeoArea].

7.1.3 MN-SET command

MN-GET and *MN-SET* are new commands that provide the access the N-Parameters from the SME. Some of N-Parameters in the network and transport layer have been specified in [rfc4022, rfc4113, rfc4293, rfc4087, rfc4295, rfc5488].

We define four new primitives for MN-SET and MN-GET as follows: *MN-SET.request*, *MN-SET.confirm*, *MN-GET.request*, *MN-GET.confirm*

7.1.3.1 MN-SET.request

The primitive *MN-SET.request* allows the SME to set N-Parameters. The parameters of the MN-SAP primitive *MN-SET.request* are as follows:

MN-SET.request (

CommandRef,
N-Param.OID,
N-Param.Value

)

On receipt of the primitive *MN-SET.request* the selected parameters shall be set at the network layer if applicable.

Name	Type	Description
CommandRef	Integer	Unique cyclic reference number of command.
N-Param.OID	MIB object	Object identifier of the N-Parameter. The Object identifier follows the specification of SMIv2 [rfc2578]
N-Param.Value	—	Value of the N-Parameter.

Table 7.1: MN-SET.request parameters

7.1.3.2 MN-SET.confirm

The primitive *MN-SET.confirm* reports the result of a previous *MN-SET.request*. The parameters of the primitive *MN-SET.confirm* are as follows:

MN-SET.confirm (

CommandRef,
N-Param.OID,
Errors.errStatus

)

This primitive is the response to *MN-SET.request* with the requested N-Parameter values in case the status is "success". Otherwise, an error code is returned in the status field. Possible error status includes "invalid N-Parameter object identifier" and "attempt to read from write-only N-Parameter". The error codes are the same as the ones used for *MI-SET* in [ISO-24102-2-Management-SAP].

Name	Type	Description
CommandRef	Integer	Unique cyclic reference number of command.
N-Param.OID	MIB object	Object identifier of the N-Parameter. The Object identifier follows the specification of SMIv2 [rfc2578]
Errors.errStatus	One octet integer	Return error code. See details in [ISO-24102-2-Management-SAP]

Table 7.2: MN-SET.confirm parameters

7.1.4 MN-GET command

7.1.4.1 MN-GET.request

The primitive *MN-GET.request* allow the network layer to request the reporting of N-Parameter values to the SME. The parameters of the primitive *MN-GET.request* are as follows:

MN-GET.request (

CommandRef,
N-Param.OID

)

This primitive is generated by the SME when N-Parameter values shall be retrieved. On receipt of the primitive *MN-GET.request* N-Parameters shall be reported to the SME.

Name	Type	Description
CommandRef	Integer	Unique cyclic reference number of command.
N-Param.OID	MIB object	Object identifier of the N-Parameter. The Object identifier follows the specification of SMIv2 [rfc2578]

Table 7.3: MN-GET.request parameters

7.1.4.2 MN-GET.confirm

The primitive *MN-GET.confirm* reports N-Parameter values to the SME. The parameters of the primitive *MN-GET.confirm* are as follows:

MN-GET.confirm (

CommandRef,
N-Param.OID,
N-Param.Value
Errors.errStatus

)

This primitive is the response to *MN-GET.request*. In the case of *Errors.errStatus* = "success", it means that the value of the indicated *N-Param.Value* is set with requested value. Possible error status includes "invalid N-Parameter object identifier" and "attempt to write to read-only N-Parameter value". The error code are the same as the ones defined for *MI-SET* in [ISO-24102-2-Management-SAP].

Name	Type	Description
CommandRef	Integer	Unique cyclic reference number of command.
N-Param.OID	MIB object	Object identifier of the N-Parameter. The Object identifier follows the specification of SMIv2 [rfc2578]
N-Param.Value	—	Value of the N-Parameter.
Errors.errStatus	One octet integer	Return error code. See details in [ISO-24102-2-Management-SAP]

Table 7.4: MN-GET.confirm parameter description

7.2 Parameters and Primitives for Path Selection

7.2.1 Existing commands of MN-REQUEST and MN-COMMAND

In ISO, MN-SAP and MF-SAP is detailed in [ISO-24102-CALM-Management], and MI-SAP is detailed in [ISO-21218:2008-CALM-Medium-SAP]. The name of primitives are formalized as *[prefix of name of SAP]-[COMMAND/REQUEST].[request/confirm]*. The prefix of name of SAP comes from initial letters of the layers of source and destination of the message. e.g. *M* stands for the management entity and *N* stands for the network layer. In the case of MN-SAP, the prefix of the primitive is *MN*. The exchange of parameters between the horizontal layers and the management entity is performed by means of two primitives such as: REQUEST is the primitive that is used as a message from the horizontal layers to the management entity. COMMAND is the primitive for the other direction.

Currently in [ISO-24102-2-Management-SAP], seven *MN-REQUEST* commands and five *MN-COMMAND* commands are specified as shown in Table 7.5. Appendix C shows the details of the existing *MN-REQUEST*s as currently specified in ISO [ISO-24102-2-Management-SAP].

MN-REQUESTs	**MN-COMMANDs**
FWTsetNot, FWTupdateNot, FWTdeleteNot, VCIcreatePeerMAC, ItssiPeerNot, STArxNot, STCrxNot,	FWTset, FWTupdate, FWTdelete, GCperiodCmd, GCstcTxCmd

Table 7.5: Current MN-REQUEST and MN-COMMAND

MN-REQUEST.request is the message from the management entity to the network layer in order to notify events. *e.g.* update of routing table entry, reception of message, and etc. *MN-REQUEST.confirm* is the acknowledgement of *MN-REQUEST.request*. Both messages are identified by message identifier called *CommandRef*. *MN-REQUEST.request* message

is sent with message identifier (*CommandRef*), the reference number of the request (*Request.No*) and the value of the request (*Request.Value*). *MN-REQUEST.confirm* is the acknowledgment of *MN-REQUEST.request*. It is sent with *CommandRef*, reference number of the request (*ReqConfirm.No*), optional data *(ReqConfirm.Value*) and error status (*ErrStatus*) which corresponds to the request message.

VCIcreatePeerMAC does not relate to path selection.

ItssiPeerNot is used for notification of "ITS State Information Data". As Appendix C lists all the parameters of "ITS State Information", it contains Station ID, Station types and the geographic information of the neighbouring ITS Station. It should be useful information for path selection, because the MN-REQUEST can be used as a notification of geographic information of the neighbouring ARs or the destination. Path selection manager can decide the path based on the geographic information.

SAMrxNot and *CTXrxNot* are used to notify the reception of "Service Advertisement Message"and "Service Context Message" for FAST protocol block. They do not fulfill the requirement described in Section 4.2.2, as they are dedicated to a network layer protocol block.

MN-COMMAND.request is the message from management to the other layer in order to request services. *MN-COMMAND.confirm* is the acknowledgement of *MN-COMMAND.request*. Both messages are identified by message identifier called *CommandRef*. *MN-COMMAND.request* is sent with the reference number of the command (*Command.No*) and the value of the command (*Command.Value*). *MN-COMMAND.confirm* is replied with message identifier (*CommandRef*) and reference number of the command (*CmdConfirm.No*) that are correspondent to the request message. The management entity can recognize the status of the message by error status (*ErrStatus*) and optional data (*MN-CmdConfirm.Value*) that is included in *MN-COMMAND.confirm* message.

FWTset, *FWTupdate* and *FWTdelete* fulfill the design requirements of the MN-SAP by same reason as *FWTsetNot*, *FWTupdateNot* and *FWTdeleteNot* described in the previous section. However update of forwarding table can only reflect the decision of path selection partially to the network layer protocol block. These MN-COMMANDs can not give proper action instruction of address selection, routing selection, nor anchor selection.

GCperiodCmd and *GCstcTxCmd* do not fulfill the requirement described in Section 4.2.2, as they are dedicated to a network layer protocol block.

7.2.2 New commands of MN-REQUEST and MN-COMMAND

In this section, we propose new *MN-REQUEST* commands and *MN-COMMAND* commands that are required for the path selection manager.

We follow the naming rules described above for the rest of this study. In the examples, "Station" and "Notification" are abbreviated to "STA" and "Not".

- Station → abbreviation "STA"
- Notification → abbreviation "Not"

Figure 7.3 gives the information flow between the path selection manager and the horizontal layers. As described in Section 5.1, the information maintained in the management entity is divided into two categories *i.e.* ITS Station information and Path information. The information is mainly obtained from MN-SAP and MI-SAP. but further information could be obtained from the ITS Station facilities (e.g. CAM, DENM, LDM). However the facilities layer is out of scope of this present study.

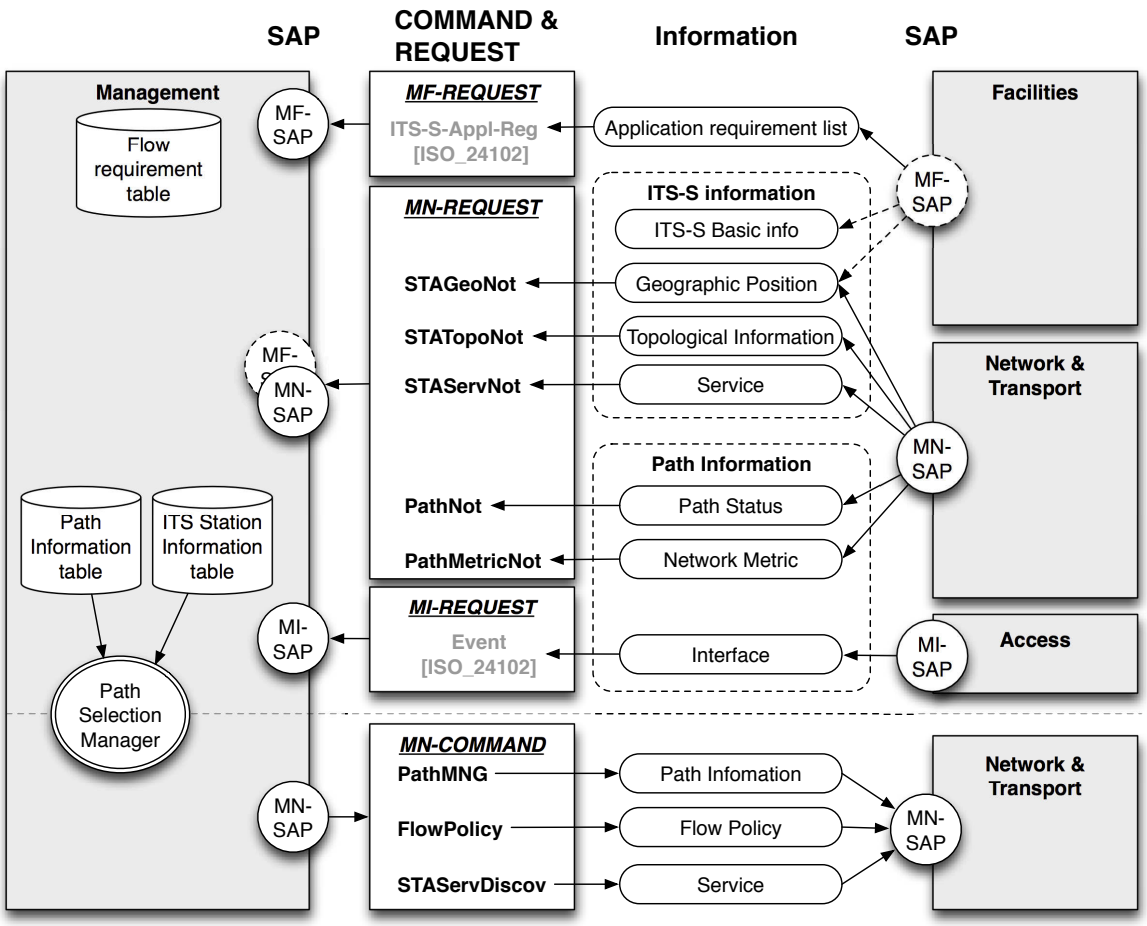


Figure 7.3: Information flow between path selection manager and the horizontal layers

We first focus on *MN-REQUEST* commands that notify the ITS Station information and Path information. As, both ITS Station information table and path information table are divided into three categories, there are six categories of information in total to be notified to the SME. However a *MI-REQUEST* command is defined as *Event* in [ISO-24102-2-Management-SAP] in order to notify the CI information of path information table. Besides, CI information from MI-SAP, there are five *MN-REQUEST* commands that notifies the network status depending on type of information are sent:

- ***STAGeoNot*** sends Geographic information of ITS Station
- ***STATopoNot*** sends Topological information of ITS Station
- ***STAServNot*** sends Service of ITS Station
- ***PathNot*** sends Path status
- ***PathMetricNot*** sends network metrics of path.

As a result of the network status notification using MN-REQUEST, ITS Station information table and Path information table are up-to-date. Also, application requirement list is updated via MF-SAP using ***ITS-S-Appl-Reg*** as defined in [ISO-24102-2-Management-SAP].

The application requirement list is maintained in the management entity in *ApplReqList*. (See details in Appendix C).

The path selection manager comprehends the network status based on the ITS Station information table and Path information table and the application requirements in the flow requirement table. The path selection manager matches the network status and application requirements in order to find appropriate path to the application. The decision is sent to the network layer as an instruction. There are three types of *MN-COMMAND* commands depending on the target of instruction.

- ***STAServDiscov*** commands service discovery,
- ***PathMNG*** commands establishment and management of paths, and
- ***FlowPolicy*** commands the flow policy to set how to use established paths

If the path selection manager finds a path that satisfies the application requirement already in the path information table, it set the flow policy using *FlowPolicy* to direct the flow to the desired path. Otherwise, the SME intervenes an action using two kinds of MN-COMMANDs. When the path selection manager needs to find other ITS Station that can provide a specific service, the SME request the service discovery to corresponding a network layer protocol block using *STAServDiscov*. When the path selection manager does not find the path that satisfies an application requirement, the SME requests the establishment of the path that satisfies the demand using *PathMNG*. The decision for CI selection, address selection, access router selection, routing selection, and anchor selection is reflected using *PathMNG*.

7.2.3 Proposition of New MN-REQUEST commands

Table 7.6 presents a summary of newly defined *MN-REQUEST* commands. A more detailed description is provided in the next sub-clauses.

Command name	Description
STAGeoNot	Notification of geographic information of an ITS Station.
STATopoNot	Notification of topological locator of an ITS Station.
STAServNot	Notification of service of an ITS Station
PathNot	Notification of status of a path
PathMetricNot	Notification of network metric of a path

Table 7.6: New MN-REQUESTs

7.2.3.1 STAGeoNot

MN-REQUEST "STAGeoNot" shall be used by the network layer adaptation agent to notify the geographical position information of an ITS Station to the SME. Table 7.7 shows the parameters of “STAGeoNot”.

7.2.3.2 STATopoNot

MN-REQUEST "STATopoNot" shall be used by the network layer adaptation agent to notify the topological locator information of an ITS Station to the SME. Table 7.8 shows the parameters of “STATopoNot”.

ASN.1 Type	Valid Range	Description
MN-Request.**sTAGeoNot**	—	Notification of geographic information of an ITS Station
STAGeoNot.**ITS-scuId**	ITS-scuId	ITS-SCU-ID of an ITS Station at the geographical position reported in the request.
STAGeoNot.**latitude**	32 bit signed integer	WGS-84 latitude of the ITS Station, that expressed in 1/10 micro degree.
STAGeoNot.**longitude**	32 bit signed integer	WGS-84 longitude of the ITS Station expressed in 1/10 micro degree.
STAGeoNot.**altitude**	16 bit signed integer	Altitude of the ITS Station expressed in signed units of 1 meter.
STAGeoNot.**speed**	16 bit signed integer	Speed of the ITS Station expressed in signed units of 0.01 meter per second.
STAGeoNot.**heading**	16 bit unsigned integer	Heading of the ITS Station expressed in unsigned units of 0.1 degrees from North.
STAGeoNot.**accuracy**	16 bit unsigned integer	Accuracy indicator of the geographical position of the ITS Station
STAGeoNot.**timestamp**	UTC	The time when the corresponding geographical position is recorded in units of seconds.
STAGeoNot.**lifetime**	16 bit unsigned integer	(Optional) The expiration time of the corresponding geographical position entry in units of seconds.

Table 7.7: Parameters of MN-REQUEST “STAGeoNot”

ASN.1 Type	Valid Range	Description
MN-Request.**sTATopoNot**	—	Notification of the topological locator of an ITS Station
STATopoNot.**ITS-scuId**	ITS-scuId	ITS-SCU-ID of the ITS Station that has the topological locator reported in the request.
STATopoNot.**locator**	64 bit integer	Topological locator of the ITS-S in the network. In IPv6, it is the network part (first 64bits) of an IP address that indicates the topological location of the node.

Table 7.8: Parameters of MN-REQUEST “STATopoNot”

7.2.3.3 STAServNot

MN-REQUEST "STAServNot" shall be used by the network layer adaptation agent to notify the service information of an ITS Station to the SME. Table 7.9 shows the parameters of “STAServNot”.

ASN.1 Type	Valid Range	Description
MN-Request.**sTAServNot**	—	Notification of the service of an ITS Station
STAServNot.**ITS-scuId**	ITS-scuId	ITS-SCU-ID of the ITS Station that provides the service reported in the request.
STAServNot.**service**	64 bit flags	The services that the ITS-S can provide. ▷ DNS server ▷ Multicast Listener ▷ Location registration ▷ QoS ▷ Gateway ▷ TBD ▷ DHCP

Table 7.9: Parameters of MN-REQUEST "STAServNot"

7.2.3.4 PathNot

MN-REQUEST "PathNot" shall be used by the network layer adaptation agent to notify the status of a path. Table 7.10 shows the parameters of "PathNot".

ASN.1 Type	Valid Range	Description
MN-Request.**pathNot**	—	Notification of status of a path
PathNot.**linkID**	Link-ID of CI	Link ID of the CI where the path starts from
PathNot.**locator**	64 bit integer	Topological locator of the ITS-S in the network. In IPv6, it is the network part (first 64bits) of an IP address that indicates the topological locator the node.
PathNot.**nexthop**	ITS-scuId	ITS-SCU-ID of an ITS Station on the path that acts as a border router when packet goes beyond the network managed by a local routing protocol.
PathNot.**anchor**	ITS-scuId	ITS-SCU-ID of an ITS Station that provides Locator registration function to ITS-S.
PathNot.**reachability**	16 bit flags	Topological distance indicator from the CI ▷ on-link ▷ ITS domain ▷ Local Network ▷ Global Network ▷ Extended Local ▷ TBD
PathNot.**capabilities**	64 bit flags	Capability of the path. ▷ Reverse reachability for host ▷ 1-to-n for group ▷ Session continuity for host ▷ 1-to-n for GeoArea ▷ Reverse reachability for network ▷ QoS ▷ Session continuity for network ▷ TBD
PathNot.**status**	16 bit flags	Status of the path. 0: not available 2: ready to be used 4: going to up 1: being used 3: potentially ready 5: going to down

Table 7.10: Parameters of MN-REQUEST "PathNot"

7.2.3.5 PathMetricNot

MN-REQUEST "PathMetricNot" shall be used by the network layer adaptation agent to notify path metrics. Table 7.11 shows the parameters of "PathMetricNot".

ASN.1 Type	Valid Range	Description
MN-Request.**pathMetricNot**	—	Notification of network metric of a path
PathMetricNot.**Payload**	0 - 65536	Size of payload for a packet using the path.
PathMetricNot.**Delay**	0 - 65536	A trip time that the path has, and actual round trip time to reach to the node in the destination scope
PathMetricNot.**Hop**	0 - 255	Number of hops to reach to the destination.

Table 7.11: Parameters of MN-REQUEST "PathMetricNot"

7.2.4 Proposition of New MN-COMMAND commands

Table 7.12 presents a summary of newly defined *MN-COMMAND* commands in this study. A more detailed description is provided in the next sub-clause.

COMMAND name	Description
PathMNG	Command for managing a path
FlowPolicy	Set flow policy for the currently available paths in self and neighbor ITS Stations.
STAServDiscov	Discover an ITS Station that can provide a service

Table 7.12: New MN-COMMANDs

7.2.4.1 PathMNG

MN-COMMAND "PathMNG" shall be used by the SME to request management of a path, that includes establishment, removal of a path or change of the path parameters (the locator, the nexthop and the anchor and etc.). Table 7.13 shows the parameters of "PathMNG".

ASN.1 Type	Valid Range	Description
MN-Command.**pathMNG**	—	Notification of status of a path
PathMNG.**linkID**	Link-ID of CI	Link ID of the CI where the path starts from
PathMNG.**locator**	64 bit integer	Topological locator of the ITS-S in the network. In IPv6, it is the network part (first 64bits) of an IP address that indicates the topological locator of the node.
PathMNG.**nexthop**	ITS-scuId	ITS-SCU-ID of an ITS Station on the path that is a border between wireless network and wired network.
PathMNG.**anchor**	ITS-scuId	ITS-SCU-ID of an ITS Station that provides Locator registration function to self ITS-S.
PathMNG.**reachability**	16 bit flags	Topological distance indicator from the CI ▷ on-link ▷ ITS domain ▷ Local Network ▷ Global Network ▷ Extended Local ▷ TBD

Table 7.13: Parameters of MN-COMMAND "PathMNG"

7.2.4.2 FlowPolicy

MN-COMMAND "FlowPolicy" shall be used by the SME to request management of flow policy in the ITS Station or the neighbor ITS Station. Table 7.14 shows the parameters of "FlowPolicy".

ASN.1 Type	Valid Range	Description
MN-Command.**flowPolicy**	—	Notification of status of a path
FlowPolicy.**applicationID**	application ID	An identifier to distinguish flow from an application. Application ID is mapped to source locator, source port, destination locator, destination port and flow type.
FlowPolicy.**pathID**	path ID	unique ID to identify a path
FlowPolicy.**dest**	ITS-scuId	ITS-SCU-ID of an ITS Station where the flow policy is injected.
FlowPolicy.**action**	16 bits flags	Action for corresponding flow (forward or drop)

Table 7.14: Parameters of MN-COMMAND "FlowPolicy"

In an example in IP, the application ID can be translated into traffic selectors for flow bindings (source address, destination address, IPsec Security Parameter Index (SPI), flow label, source port, destination port, traffic class and next header) specified in [rfc6088]. The network layer applies the rule. The IPFilter[1] is common tools to set the filtering rule. To apply a rule to inbound traffic, the SME specified the destination parameter as a neighbor ITS Station in order to send the flow binding request to update the rule of neighbor ITS Station (*i.e.* MR, HA or CN). For example, the flow binding can be delivered by extended BU specified in [rfc6089] in Mobile IPv6 and NEMO case, or more generic ways (ex. https) for the other mobility management modules as in [draft-larsson-mext-flow-distribution-rules]. See details for Flow Binding in Section 3.5.4.

7.2.4.3 STAServDiscov

MN-COMMAND "STAServDiscov" shall be used by the SME to request service discovery. Table 7.15 shows the parameters of "STAServDiscov".

ASN.1 Type	Valid Range	Description
MN-Command.**sTAServDiscov**	—	Discover an ITS Station that can provide a service
STAServDiscov.**service**	64 bits flags	The services that the ITS-S can provide to self ITS-S. ▷ DNS server ▷ Multicast Listener ▷ Location registration ▷ QoS ▷ Gateway ▷ TBD ▷ DHCP

Table 7.15: Parameters of MN-COMMAND "STAServDiscov"

For example, in the IPv6 protocol block of the network layer, the service discovery triggers Router Solicitation, Neighbor Solicitation in NDP to discover new ARs and new neighbors when service field is specified as discovery of "access" and "neighbor". Or Anchor service

[1] http://www.netfilter.org

discovery is specified in service field of *ServDiscov*, it is translated into Dynamic Home Agent Address Discovery request in NEMO. The cycle of the path selection manager returns to the candidate path calculation described in Section 6.2.1, because another candidate path may appears as a result of service discovery (*e.g.* discovery of new access services (ARs) or anchor services).

7.3 Mapping of Management and Network layer Parameters

7.3.1 Adaptation Agent

In this section, we describe the mapping between the abstracted databases (ITS Station information table and path information table) shown in Section 6.1 and concrete database in the network layer protocol blocks (IP, GeoNetworking and FAST). The adaptation agent translates concrete parameters in the network layer into abstracted parameters, when it sends the *MN-REQUEST*. On the other hand, the adaptation agent translate the abstracted parameters from the management entity into concrete parameters in the network layer on the reception of *MN-COMMAND*.

The detailed formats of parameters and examples are also shown in the following sections.

7.3.2 ITS Station information table

Table 7.16 shows the mapping between the parameters of the ITS Station information and the corresponding parameters maintained in the network layer. The tables shows the database that the corresponding parameters are stored in the network layer and how to they are obtained.

The three types of information (topological information, geographic information, and service information) about neighbor ITS Station are linked to a Station ID. Although the format of Station ID is not specified yet, we propose 64 bits address. We propose that the 64 bit of Station ID corresponds to IPv6 prefix used at the IPv6 layer as the ITS Station internal network prefix. Because, both Station ID and the Station internal prefix have to be a globally unique identifier and that should be permanently allocated. In IPv6 case, the Station internal prefix corresponds to network prefix, or mobile network prefix (64bits). Type of ITS Station (e.g. vehicle, roadside, central and personal) is basic information, however the parameters are not registered in database nor exchanged. Vehicle type is stored in Local Dynamic Map (LDM) and can be optionally exchanged by Decentralized environmental Notification Messages (DENM) in the facilities layer.

In the case of the Internet, the topological locator is expressed with first 64 bit of the IPv6 address that is called network part of the address (last 64 bits is the CI identifier). At the network layer, some IP addresses of the ITS Station are stored in the routing table in IP block. It can be exchanged, for example, by messages of Neighbor Advertisement (NA), Router Advertisement (RA) and DHCP. In some mobility management modules, the identifier and the topological locator are managed as different IP addresses. For example, in NEMO, the identifier of an MR is the HoA and the topological locator is the CoA. On the other hand, the topological locator of the MNN is the network part of the MNP of the MR that attaches to.

About geographic information, GeoNetworking maintains the position (latitude, longitude and altitude) and the movement information (speed and heading) of the neighbor ITS Stations with the accuracy indicator and the time stamp in the location table. These parameters are

Management Parameters		Corresponding Parameters in the network layer	How it obtained in the network layer
Basic	Station ID	Used also as the Station internal prefix. *i.e.* MNP	Exchanged by MNPP and DENM message
	Station type	TBD	TBD
	Vehicle type	(Maintained in LDM in the facilities layer)	(Carried by DENM message optionally)
Topological	Locator	Maintained in the routing table as a IP address	Exchanged by Neighbor Advertisement, Router Advertisement, and DHCP
Geographic	Position	Maintained in the location table, (or LDM) depending on the configuration	Exchanged by Beaconing, Location Service (and DENM message)
	Movement		
	Accuracy		
	Time stamp		
	Distance	The distance to a neighbor ITS Station can be calculated by the positions of two ITS Station. i.e. *Haversine* formula	
	Estimated Connection	The estimated connection time to a neighbor ITS Station can be calculated by movement prediction	
Service	Locator registration	ITS-Ss provide the service are kept in HA list in NEMO	The service is exchanged by DHAAD request and DHAAD reply
	Access	ITS-Ss provide the service are kept in the routing table as default gateway	Notified by Router Advertisement and DHCP
	FAST service	Service in FAST is stored in *servContextList*	Carried by Service Context Message

Table 7.16: Mapping of the ITS Station information to the network layer protocol blocks parameters

exchanged by the beaconing and the location service. Alternatively, in the facilities layer, LDM stores the position and the movement information of the neighbor ITS Stations and DENM exchanges the information.

The service field is a set of flags that indicates the service that could be provided by the neighbor ITS Station. The relation can be client and server of some service. Here, let's take three examples of services. The "locator registration" service is provided by an HA in NEMO and vehicle ITS Station has the information in HA list in the network layer. The information can be obtained by Dynamic Home Agent Address Discovery (DHAAD) request and DHAAD reply. On the other hand, an AR provides the "access" service in the IP networks. An ITS Station can discover the AR by Router Solicitation (RS), Router Advertisement (RA) or DHCP messages. The results of the messages are often stored as a default gateway in the IP routing table. In FAST, service context are defined and stored in the database called *servContextList*. The service context is exchanged by Service Context Message.

As an ITS Station can provide several services, the multiple flags of service field can be marked at the same time. Since an ITS may provide multiple service, the service information is recorded with 64bits flags. The other flags are reserved for future usage. The service can

be discovered by the service discovery mechanism located in any layer.

7.3.3 Path Information table

The management entity stores path information that is received from the access layer and the network layer. The three classes of path information that are CI, Path status and Metric as shown in Table 7.17.

Management Parameters		Corresponding Parameters in the network layer	How it obtained in the network layer
CI	CI parameters	The parameters is provided from MI-SAP. *e.g.* Media type, Data rate, Cost and Reliability	
Path Status	Locator	Maintained in the routing table as a IP address	Exchanged by NA, RA, and DHCP
	Next hop	Maintained in the routing table as default gateway	Obtained from RA and DHCP
	Anchor	Maintained in HA list in NEMO	Obtained by DHAAD, BU and BA.
	Reachability	Determined by the types of IP address, or maintained in routing table	IP address is obtained by RA and DHCP. Route is exchanged by MNPP.
	Capabilities	"reverse reachability" capability is maintained in BUL and BC in NEMO	Exchanged by BU and BA
	Status	Calculated by Path Availability Estimation in the management entity as described in Section 6.2.2	
	Start time		
	End time		
Metric	Payload size	Calculated by MTU and encapsulated headers	
	Delay	Some measurement is necessary	
	Hop	Some routing protocol provide the information	

Table 7.17: Mapping of the Path information to the network layer protocol blocks parameters

The CI information have big impact to the correspondent path as a starting point of the path. They are provided from the interface between the management entity and the access layer (MI-SAP). *i.e.* Media type, data rate, reliability and etc (See Section 6.1.2).

Path status includes the parameters that characterize the path. In the case of the Internet, the topological locator corresponds to network part (first 64 bits) of the IP address configured to the CI. Multiple locators can be configured to the CI at the same time and in such case, the path selection manager considers that these are different paths. The topological locator is stored in the routing table and for example, exchanged by Neighbor Advertisement (NA), Router Advertisement (RA) and DHCP.

In the Internet-based communication, an AR is the "next hop" of the path. The "next hop" is also maintained in the routing table as a default gateway and can be obtained by RA and DHCP. The next hop is an AR in the case where the correspondent path goes to infrastructure, and it is an MR in direct V2V communication.

In the NEMO mobility management module,, the "anchor" corresponds to the HA. The HA address is maintained in the HA list and can be obtained by Dynamic Home Agent

Address Discovery (DHAAD), Binding Update (BU) and Binding Acknowledgement (BA). Anchor field indicates neighbor ITS Station provides a location registration service to mobile ITS Station to support mobility. The "Next hop" and "anchor" parameters are linked to an entry of the ITS Station information table.

The reachability of the path is often determined by the types of the address. In IPv6, link-local address and global address correspond to the "on-link" and "Global Network" reachability, respectively. Some reachability information is also maintained in the routing table. For example, the routing entries added by some routing protocol indicate the reachability to the network. "Local Network" reachability is enabled by VANET routing protocols (*e.g.* GeoNetworking). "Extended Local" reachability is obtained by Mobile Network Prefix Provisioning (MNPP) by obtaining the route to the ITS Station internal prefix.

For example, as a "capability", reverse reachability of the path is acquired by the locator registration to an anchor. In NEMO, reverse reachability capability is acquired by the message exchange of BU and BA between HA and MR. The result of the message is stored in BUL in NEMO. QoS, multicast for group and multicast for GeoArea are also examples of the capabilities. The path can have multiple capabilities at the same time, thus the multiple flags of capabilities can be marked at the same time.

In the metrics field, payload size, propagation delay and number of hops are the parameters for the path status. Payload size is determined with MTU and header size. For example, in the case that the path is established with GeoNetworking, IP and NEMO over Wifi interface, the *payload* size is 1340 Bytes and can be calculated by equation 7.1, where MTU of wifi interface is 1500 Bytes, header size of $GeoNetworking$ is 80 Bytes, header of IP is 40 Bytes, and header of $NEMO$ encapsulation is 40 Bytes.

$$Payload = MTU–GeoNetworking–IP–NEMO \tag{7.1}$$

To obtain the propagation delay, same measurement is needed, and the number of hops is obtained by measurement, or provided by some routing protocol.

7.4 Network-Management Interaction for Path Management

7.4.1 Procedure

Figure 7.4 shows how path selection is performed from the moment that a CI becomes available. Numbers on the arrows indicates the message between the SME and the data plane. The numbers from (1) to (4) show the message via MI-SAP, and the numbers from (5) to (13) show the interaction via MN-SAP. The procedure progresses basically from bottom to top in the ITS Station architecture.

[ISO-21218:2008-CALM-Medium-SAP, ISO-24102-2-Management-SAP] describe the initial part of the procedure and message exchange via MI-SAP.

(0) A CI's power is turned on

(1) The Interface Management Entity (IME) registers the CI identified by an unique identifier, and the Communication Interface Management Adaptation Entity (CIMAE) notifies the event to the SME using *RegReq*.

(2) IME may perform "Cross-CI prioritization" as an optional procedure to synchronize transmission of multiple CIs based on user priority. The event is notified from CIMAE to the SME using *PrioReg*.

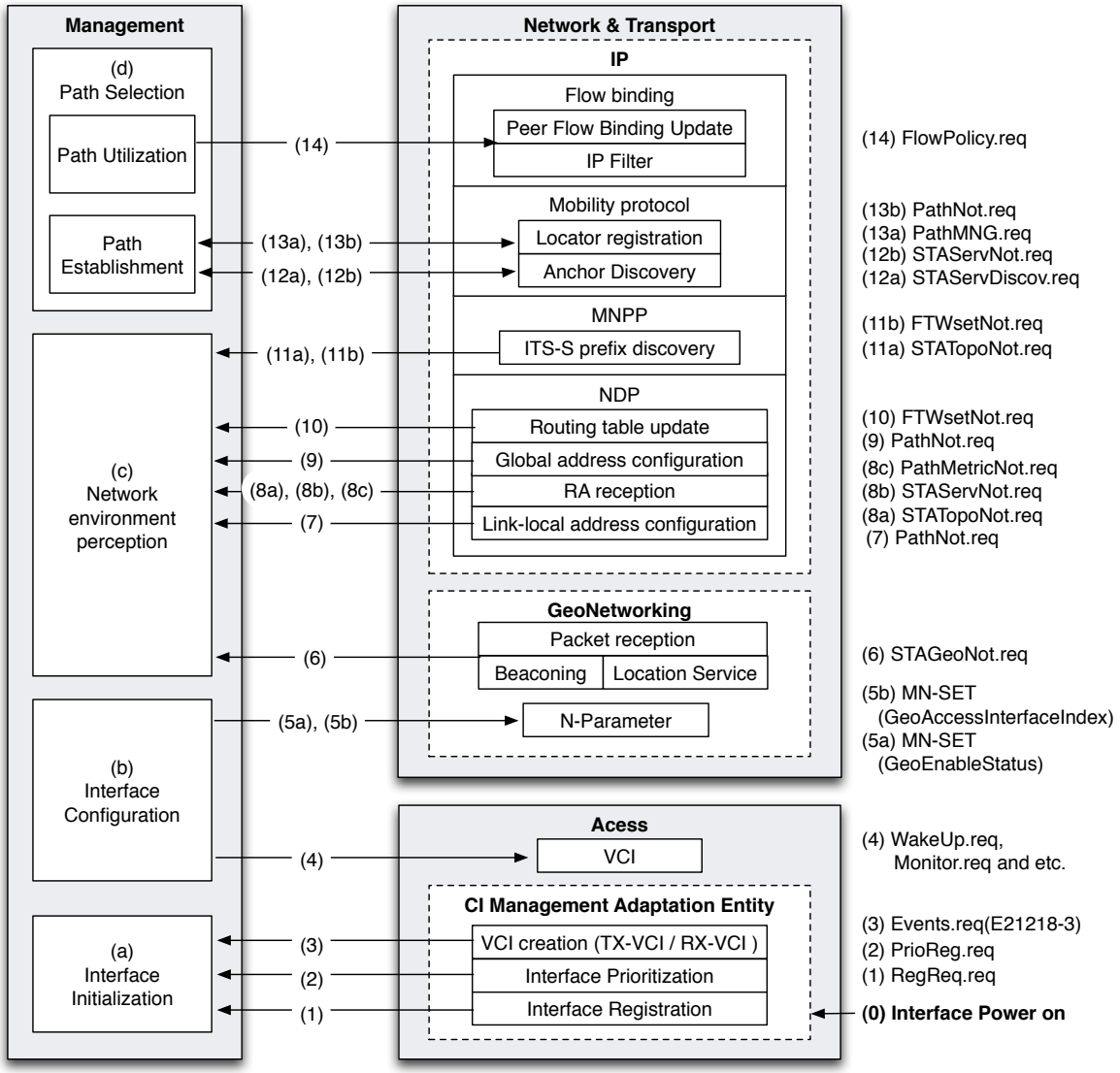


Figure 7.4: Procedure of Path Management

(3) A TX-VCI and an RX-VCI shall be created by the CIMAE based upon the default MIB. Parameter 42 "CIstatus" shall be set to "active". The event is notified from the CIMAE to the SME using *Events.req(E21218-3)*.

(4) Once VCIs are created, the SME can send MI-COMMAND to the corresponding VCI. For example, *Wakeup* starts repetitive transmission of wake-up signal with maximum interval in milliseconds. *Monitor* requests monitoring of CI parameters.

Some of the messages exchanged via MN-SAP from (5) to (13) are defined in Section 7.2 in the thesis and others are defined in [ISO-24102-2-Management-SAP].

(5a) If GeoNetworking is disabled, the SME can activate GeoNetworking by setting *GeoEnableStatus* (N-Parameter) using *MN-SET*. If GeoNetworking is already running or GeoNetworking is not used, this step is skipped. N-Parameters for GeoNetworking are specified in Section 7.1.2.

(5b) In the case where GeoNetworking is used over the created VCIs, the VCIs is set as *GeoAccessInterfaceIndex* in N-Parameter for GeoNetworking using *MN-SET*.

(6) When GeoNetworking is enabled, there are three ways to obtain the geographic information of neighbor ITS Station: beaconing, location service and packet reception. Every GeoNetworking packet has a common header that includes source nodes's geographic information. The information is notified to the SME using *STAGeoNot*. Note that, if GeoNetworking is not used, geographic information of neighbor ITS Stations cannot be obtained from the network layer. Alternatively, it could be obtained through the Local Dynamic Map at the facilities layer.

(7) The IPv6 Link-local address on an egress interface (VCIs or GeoNetworking interface) is configured. *PathNot* notifies that on-link "reachability" is enabled from the egress interface. Topological locator field is left as empty, because network part of link-local address (*fe80*) does not indicates the topological location.

(8a) On reception of a Router Advertisement from a roadside ITS Station, the system receives the topological locator information of the roadside ITS Station. The information is sent to the SME using *STATopoNot*. Note that the system may receive geographic information of the station at the same time, when the Router Advertisement is encapsulated into GeoNetworking packet. See step (6) for this case.

(8b) At the same time on the reception of the Router Advertisement, the system also detects that the neighbor ITS Station provides a access service. The service capability of the ITS Station is notified to the SME using *STAServNot*.

(8c) The Router Advertisement may contain the MTU size of the access network as a Router Advertisement option. In this case, the MTU size is notified to the SME using *PathMetricNot*.

(9) A Global address is configured on the received egress interface on the reception of a Router Advertisement. The SME notifies the acquisition of Global Network "reachability" from the egress interface with the topological locator which is the 64 bits network part of the acquired global address using *PathNot*.

(10) A default gateway is added or updated to the routing table on the reception of a Router Advertisement. Then the update is notified to the SME using *FWTsetNot* or *FWTupdateNot*.

(11a) Eventually, an Mobile Network Prefix Provisioning (MNPP) advertisement is received. From the message, the IPv6 obtains a new CoA (*i.e.* topological locator) and ITS Station internal IPv6 network prefix of the neighbor ITS Station (*i.e.* the neighbor ITS Station ID). The information of the neighbor ITS Station is notified to the SME using *STATopoNot*.

(11b) On reception of MNPP advertisement, a route to the neighbor ITS Station prefix is created in the routing table. The update of the routing table is transmitted to the SME using *FWTsetNot*.

(12a) Once a global address is configured on an egress interface, it has to be registered to an anchor to support mobility. When there is no available anchor recorded in the ITS

Station information table, the SME can request service discovery of anchor service to the mobility management module using *STAServDiscov*.

(12b) As a result of anchor service discovery (In NEMO case, DHAAD is the service discovery), the mobility management module obtains a list of anchors. The anchor list is sent to the SME using *STAServNot*.

(13a) The SME requests IP to registers the topological locator with an anchor based on the path selection decision using *PathMNG*. The CI selection, address selection, access router selection and anchor selection are reflected as a result of the MN-COMMAND.

(13b) The status of locator registration (*e.g.* Binding Acknowledgement or Binding Error) is notified from the mobility management module to the SME using *PathNot*. From the MN-REQUEST, the SME updates the path information kept in the SME.

(14) When multiple paths are available to the destination, the SME can request to inject a flow policy using *FlowPolicy*. The flow policy may be applied to local IP Filter or to an anchor's IP filter with peer flow binding update.

Although the SME performs (a) CI initialization and (b) CI configuration, it manages the cycle of (c) network environment perception and (d) path selection at the same time.

7.4.2 ITS Station information management

This section describes how topological information, geographic information and service information are corrected at the ITS Station network and transport layer to the management entity.

7.4.2.1 Topological information

The IP layer provides topological information of the other ITS Stations to the SME. ITS Station detects the movement by finding new network by NDP. MR sends Router Solicitation to all router multicast (ff02::2) in order to find ARs around the vehicle. In IPv6 GeoNetworking, the multicast packet is delivered over GeoBroadcast as described in Section 8.5. AR sends Router Advertisement on demand or periodically to all node multicast (ff02::1), that transmitted over GeoBroadcast. On the reception of a Router Advertisement at MR, it detects the movement. When MR receives a Router Advertisement, IP sent AR's address (source address of the Router Advertisement) to the SME using *STATopoNot* as the topological locator (See Section 7.8 for details). As well as reception of Router Advertisement, MR obtains topological information of the ITS Station on the reception of Neighbor Advertisement and it is notified to the SME as the topological locator using *STATopoNot* as well.

MR also sends MNPP solicitation and receives MNPP advertisement. The messages are delivered with all router multicast using GeoBroadcast and with *all node multicast* using GeoBroadcast, respectively. MNPP advertisement also tells ITS Station network prefix information in addition to the topological locator of the ITS Station. Both ITS Station network prefix information and topological locator are notified to the SME using *STATopoNot*.

The topological information is sent from the network layer to the SME using *STATopoNot*, when a network layer protocol block finds a new neighbor ITS Station. For example, when new CN appears and inbound and outbound packet are forwarded to the MR, the MR discovers a new neighbor ITS Station that communicates with itself Station and the information is sent to the SME using *STATopoNot*.

7.4.2.2 Geographic information

In the GeoNetworking protocol block of the ITS Station network and transport layer, each ITS Station maintains location of the other ITS Stations in the database called location table, in order to forward the packet with geographic routing. Each entry of the location table has GeoNetworking ID, latitude, longitude, altitude, speed, heading and lifetime as mentioned in Table 3.3. When an entry is added or updated, the event is notified to the SME using *STAGeoNot*. Also, when the lifetime of the location table entry expires, GeoNetworking notifies that the entry is removed via *STAGeoNot*. When a location table entry is removed, the parameter of *STAGeoNot* (See Section 7.2.3.1) set as "unknown" except for the GeoNetworking ID and the time stamp. The management entity updates the geographic information of the ITS Station information accordingly in both cases.

There are three main ways to update the location table upon the reception of GeoNetworking packets:

- Reception of beacon
- Reception of location service
- Reception of GeoNetworking packet (*GeoUnicast, GeoBroadcast, GeoAnycast, TopoBroadcast*)

First, the GeoNetworking nodes regularly exchange location information by one hop beaconing (Interval of beacons is 0.5 second in default). Seconds, when a node needs to know the position of a node more then one hop away, the location service is used. Location service requests the location information of the target node by GeoNetworking ID in term of request-reply manner with multi-hop communication. Then, the location table can be updated when a packet is received, because the GeoNetworking header includes the source node location information.

To enable roadside-based and Internet-based communication, a vehicle ITS Station needs to discover a roadside ITS Station discovery. The current specification of GeoNetworking does not provide means to distinguish vehicle ITS Station and roadside ITS Station from the message. However, in IPv6 GeoNetworking, we can assume that a router that sends Router Advertisement is a roadside ITS Station. The receiver of the Router Advertisement can uniquely identify the GeoNetworking ID and the Router Advertisement, because the GeoNetworking ID of Router Advertisement and the last 64-bits of AR's link-local address are identical.

The three ways above also allow to discover the AR's position from GeoNetworking packets, because AR is considered as fixed GeoNetworking node. In addition to these three ways, there is one more way to know AR's position which is:

- History-based / Map-based AR discovery

where the ITS Station discover ARs by downloading from the server or by reading from DVD-ROM.

Geographic information is sent from the network layer to the SME using *STAGeoNot*, when a network layer protocol block finds a new ITS Station's geographic information. For example, a DNS-like location service may be able to resolve the geographic position of a central ITS Station. Result of such services is sent to the SME using *STAGeoNot*.

7.4.2.3 Service Information

The management entity maintains also service information in the ITS Station information table. The information about services provided by neighbor ITS Station is recorded in service field in ITS Station information table. Service includes access, location registration, DNS, multicast listener, QoS and so on. Service field leave rooms for future extension.

On the reception of Router Advertisement, a vehicle ITS Station notices that the AR (source of the Router Advertisement) of a roadside ITS Station can be used as a gateway to other networks. Then NDP sends the information that the roadside ITS station has "access" service to SME using *STAServNot* (See Section 7.9 for details). Also, when some Router Advertisement option is attached to the Router Advertisement, the receiver may notice other services. For example, Router Advertisement can advertise DNS recursive server addresses to the receiver with Router Advertisement option as specified in [rfc6106]. Or in HMIPv6 case, a Router Advertisement option carries address information of MAP [rfc5380] (MAP is treated as a node that provides locator registration service as mentioned later in this section). On the contrary, when the decision needs to discover such services, the SME requests *STAServDiscov* to the network layer (See Section 7.15 for details) to the network layer to discover the service. The network layer actually sends Router Solicitation to *all router multicast* address to find a router which advertise these service.

Instead of Router Advertisement, DHCPv6 can provide to the vehicle ITS Station which node has access service and DNS service. DHCP is also one of the services, thus the DHCP server is recorded as the neighbor ITS Station provides DHCP service. The service information which are obtained by DHCPv6 (access, DNS and also DHCP) are sent to the SME using *STAServNot* as well. The SME can request service discovery to the network layer using *STAServDiscov*.

To support mobility, MR should find at least an anchor to register a topological locator of the MR. To the discover anchor provides a locator registration service, the SME requests to the network layer using *STAServDiscov* to perform service discovery. MR may perform the service discovery of locator registration when no anchor is found yet or none of candidate anchors is favorable. As a response of the service discovery, MR get a list of anchors, and the service information is sent to the SME using *STAServNot*. In the case of NEMO, the service discovery request of locator registration is translated to DHAAD request and the reply is translated to DHAAD reply.

7.4.3 Path information management

ITS Station manages all the candidate paths and the metric in path information (See Section 7.3.3) in the management entity. This section describes how CI information, path status and path metric are managed within IPv6 GeoNetworking.

7.4.3.1 CI Information

CI information has big impact to determine the characteristics of the corresponding path as the end point of the path. The SME accesses VCI to obtain the CI information fields of the path information table via MI-SAP. There are three ways to access a VCI via MI-SAP.

1. Using MI-GET to get a parameter of VCI. The SME initiates the message and identifies the VCI parameters by "*I-Param.No*". By specifying the parameter from *"I-Param.No"=0* to *"I-Param.No"=51*, the SME can get the value of all the necessary

parameters for CI information of the path information table. This is used when the SME gets the CI information on demand.

2. Using MI-REQUEST "*Event*" to get the notification of an I-Parameter value. MI-REQUEST is initiated by the access layer to the SME. This is used when the SME gets the CI information of the path information table immediately after an event.

3. Using MI-COMMAND "*Monitor*" to start and stop monitoring a specific I-Parameter. Contrary to MI-REQUEST, MI-COMMAND is initiated by the SME to the access layer, this is used when the SME gets specific I-Parameter during a certain period of time.

The SME updates the CI information in the path information table according to the notification with any of the three ways described above.

7.4.3.2 Path Status

The network layer does not have a complete list of the paths, thus only available paths are identified by a unique ID in the network layer. In MCoA case, BID is used as the unique ID.

While an available path is notified by *PathNot*, a possible path is calculated in the management entity using the Possible path calculation function described in Section 6.2.1. The result of the calculation is stored in the path information table. "Start time" and "end time" fields of the path information table are filled by the path availability estimation function in the management entity described in Section 6.2.2.

7.4.3.3 Path Metric

The performance of a path deeply depends on characteristic of the CI, path status and also the network metrics. The examples of the path metrics are:

- Payload size
- Delay
- Hop count

The metric may be provided by the network layer to the SME using MN-REQUEST "*PathMetricNot*" (See Section 7.2.3.5 for details), or be provided by other measurement means.

The payload size can be determined from the MTU size and the header size of the protocol. *i.e.* NEMO or GeoNetworking. For example, the MTU of the access link is provided by the Router Advertisement option. NEMO and GeoNetworking add 40 bytes and 80bytes as NEMO header and GeoNetworking header, respectively. The information is notified from the network layer to the SME using MN-REQUEST "*PathMetricNot*". The management entity can calculate the payload size of the information.

The path delay can be measured by the RTT of the mobility signaling in the NEMO case. The information is reported from the network layer to the SME using *PathMetricNot*.

Some VANET protocols can provide hop count to the nodes that join in the network. The metric can be notified to the SME and stored in path information table.

Any of the above metrics can be left as empty when the metric is unknown.

Chapter 8

IPv6 GeoNetworking

Contents

In this chapter, we present the mechanisms allowing the combination of IPv6 and GeoNetworking according to the requirements expressed in Chapter 4. First, we review the functional modules and the interfaces between the entities composing the IPv6 GeoNetworking architecture as it was defined in the GeoNet Project. Following the approach presented in Chapter 5, the GeoNetworking module is defined as a sub-layer of IPv6. GeoNetworking therefore appears as an access layer and is presented to IPv6 in the form of a Communication Interface (CI) with GeoNetworking capabilities. The IPv6 packets delivered in a VANET where GeoNetworking is used as a multi-hop routing protocol are thus encapsulated into a GeoNetworking packet by the ITS Station router which is responsible for communication of the entire ITS Station and is managing GeoNetworking transparently to the ITS station hosts. An network layer internal interface is needed to transmit packets between IPv6 and GeoNetworking. We thus specify the GeoIP Service Access Point (GeoIP-SAP) between GeoNetworking and IPv6. In the GeoIP SAP, IPv6 packets are mapped to one of the four GeoNetworking communication types (e.g. *GeoUnicast*, *GeoBroadcast*) depending on the destination IP address. Finally, in order to alleviate the constraints that an IPv6 subnet is restricted to a geographic area, we propose the end based geographic link model. In the proposed link model, the IP address used to the roadside-based communication mode is determined by each vehicle ITS Station with more precise vehicle's information.

8.1 Functional modules and SAPs

Figure 8.1 shows the functional modules and SAP related to IPv6 GeoNetworking.

Initially, the IPv6 GeoNetworking has been developed under the framework of the GeoNet Project (from 2008 to 2010, See Section 2.1.2.1) that follows the C2C-CC architecture. However, since the ITS Station architecture is a standard architecture today, we present this work in the ITS Station architecture in this chapter. Our contributions for the project was developing IPv6 and Geo-IP SAP, thus we mainly focus on these parts in this chapter. This work have been published in [GeoNet-D.2, Tsukada2009, Tsukada2010b], and some results of this work can be seen in ETSI standards [ETSI-TS-102-636-3-GeoNetworking-Arch, ETSI-TS-102-636-6-1-IPv6-GeoNetworking].

The main difference from the C2C-CC architecture related to IPv6 GeoNetworking is the definition of the IP layer and the GeoNetworking layer. The ITS Station architecture has the IPv6 module and the GeoNetworking module in the network and transport layer whereas the C2C-CC architecture has the independent IPv6 and GeoNetworking layers. As a result the difference, the interface between IPv6 and GeoNetworking (called GeoIP-SAP) is defined as a layer-internal SAP in the ITS Station architecture and as an inter-layer SAP in the C2C-CC architecture.

The IPv6 module interacts with the lower layers either via the GeoIP-SAP or via the NI-SAP. The GeoIP-SAP is used in the case that the IPv6 module passes the packet to the egress interface, and The NI-SAP is used to pass the packet to the ingress interface.

In the IPv6 module, there are three sub-modules (IP Forwarding, mobility support and multicast). The IPv6 over GeoNetworking is the sub-modules that passes the packets to the GeoIP-SAP with required parameters in the GeoNetworking module (See details in Section 8.5). NEMO and MCoA is used to support mobility in IPv6 GeoNetworking. The IP multicast module support for IPv6 nodes to send the packet to the classical IP multicast scope and also to a geographic area as an additional valid scope with help of the GeoNetworking module.

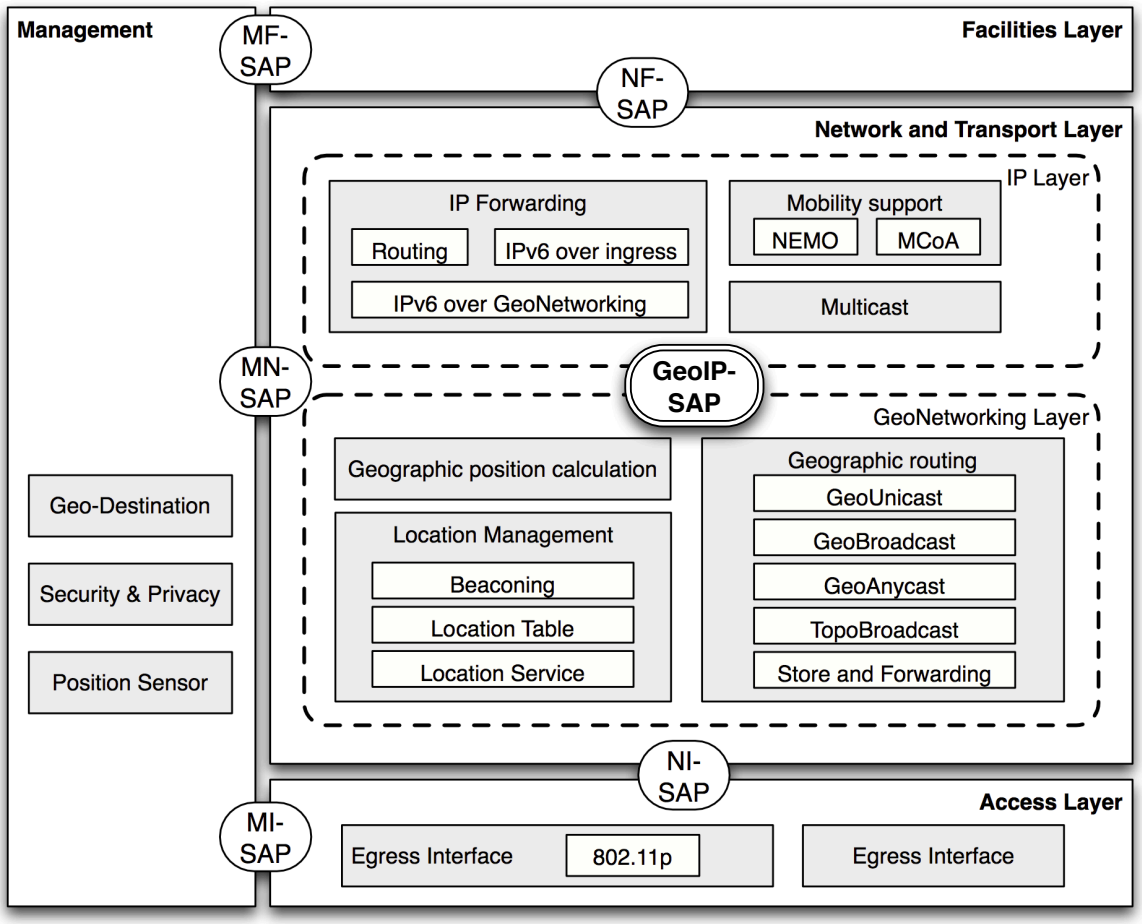


Figure 8.1: GeoNet main functional modules and SAPs

The GeoNetworking module consists of three sub-modules (Geographic position calculation, location management and geographic routing). The location of the neighbor GeoNetworking nodes are exchanged by beaconing and location service and stored in the location table in the location management sub-module. The geographic routing module enables all the communication types described in Section 3.3.2.2 such as *GeoUnicast*, *GeoBroadcast*, *GeoAnycast* and *TopoBroadcast*.

In the access layer, there are two modules. The ingress interface links to the other hosts in the same ITS Station subnet, on the other hand, the egress interface links between different ITS Stations. For well-known ingress interface such as Ethernet, existing specification can be used without modification. Alternatively, any other access technologies can be used. Only ETSI ITS G5 and IEEE 802.11p are considered in the scope of the GeoNet project, but other media could be supported likewise.

IPv6 GeoNetwork is transparent to the upper layer than the network and transport layer. Thus the upper layer is mostly out of focus in the work presented in this Chapter.

However GeoNetworking-aware applications need to specify the geographic area where the packets shall be transmitted to (GeoDestination). The GeoDestination module exists in the management entity in order to exchange the geographic area between GeoNetworking-aware applications and the GeoNetworking modules. The Security and Privacy module is

responsible to the security and privacy concerns that are specific to IPv6 GeoNetworking. The position sensor module in the management entity provides the geographic information to all the layer. GPS or the other positioning system can be used as the position sensor module.

8.2 Routing

IPv6 GeoNetworking must support all type of communications: vehicle-based, roadside-based and Internet-based (See Section 2.2.3 for details). The issues and the requirements for IPv6 GeoNetworking are discussed in Chapter 4.

Vehicle-based communication is illustrated in Figure 8.2. The ITS Station router that acts as a gateway connecting the network to other vehicle and the roadside is responsible for GeoNetworking location management and routing. ITS Station router thus encapsulates the IPv6 packets from ITS Station hosts with GeoNetworking header. The GeoNetworking encapsulated packets are transmitted in a multi-hop manner to the destination (intermediate ITS Station router are not concerned about IP routing). The ITS Station hosts do not have GeoNetworking functionality, because they are embedded nodes which have minimal resource without GPS device. *e.g.* sensor node (See this requirements in Section 4.2.5).

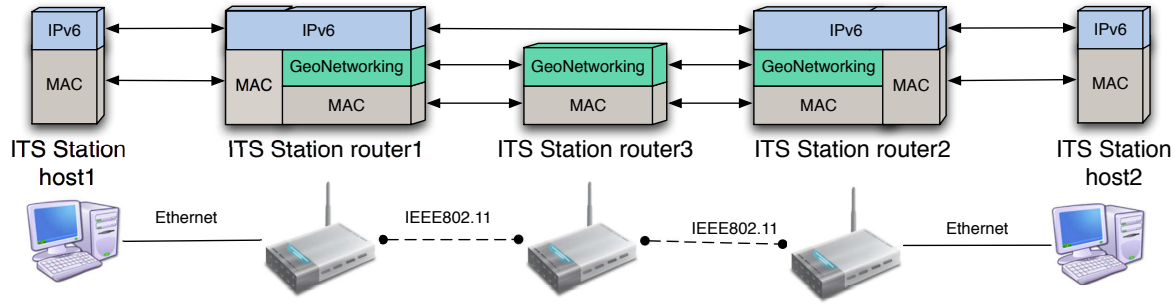


Figure 8.2: GeoUnicast in vehicle-based communications

The roadside-based communication case is shown in Figure 8.3. Vehicle ITS Station hosts should be able to communicate with any CN in the Internet and be accessible from CN in the Internet. Internet connectivity is provided through ITS Station router via any wireless media with GeoNetworking. To provide on-the-move and uninterrupted Internet connectivity, NEMO is specified by the IETF and recommended by the ISO TC204 WG16 standard [ISO-21210:2011-CALM-IPv6]. The IP packet is first encapsulated in a NEMO tunnel by the vehicle ITS Station router. Then the packets are delivered by GeoNetworking to the roadside ITS Station router. The ITS Station router decapsulates the GeoNetworking header and the IP packet is forwarded to the Internet. Since the IP packet is still encapsulated into a NEMO header, the packet reaches the HA. After the NEMO header of the IP packet is removed at the HA, the IP packet is delivered via normal IP routing to the CN.

8.3 Interface Management

MR has at least one GeoNetworking egress interface. In addition, as it is using NEMO Basic Support for maintaining the Internet reachability, it has another one for the NEMO tunnel over the GeoNetworking interface. Additional egress interfaces may be available such as standard WLAN or 3G interfaces. In addition, it has an ingress interface if it has attached

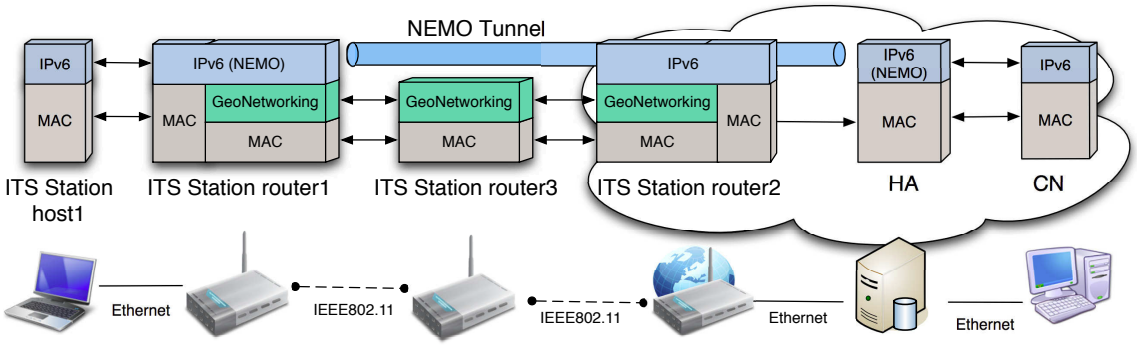


Figure 8.3: GeoUnicast in roadside-based communication

nodes. Thus the routing table of an MR must be able to maintain several types of interfaces as follows (see Figure 8.4):

(a) GeoNetworking egress interface is a tunnel interface: the packets are passed to the GeoNetworking layer and therefrom encapsulated with a GeoNetworking header. They are then passed to the access layer where they are encapsulated with an IEEE802.11p MAC header and actually emitted on the air. The GeoNetworking interface is thus recognized as a tunnel interface by the IP layer.

(b) NEMO tunnel over GeoNetworking interface is a tunnel interface: the packets are first encapsulated with an IPv6 header (source address: CoA, destination address: HA address). Then the packets are encapsulated with a GeoNetworking header. Finally they are passed to the access layer where they are encapsulated with an IEEE802.11p MAC header and actually emitted on the air.

(c) NEMO tunnel over other egress interfaces is a tunnel interface: the packets are first encapsulated with an IPv6 header (source address: CoA, destination address: HA address). The packets are passed to the corresponding access layer of the egress interface and therefrom encapsulated with MAC header of the link type and emitted on the link.

(d) Other egress interfaces are 'normal' interfaces: the packets are passed to the corresponding access layer of the interface and therefrom encapsulated with a MAC header of the link type and emitted on the link.

(e) Ingress interface is a 'normal' interface: the packets are passed to the ingress interface and therefrom encapsulated with a MAC header of the link type and emitted on the link.

On the other hand, the roadside ITS Station router does not support NEMO and has no NEMO tunnel interfaces. The interface management is thus simplified.

8.4 Address auto-configuration

Each GeoNetworking egress interface of an MR or AR must be configured with two different IPv6 addresses: a link-local address and a global address. All nodes attached to the same IPv6 GeoNetworking link should be reachable using both addresses, while the global address

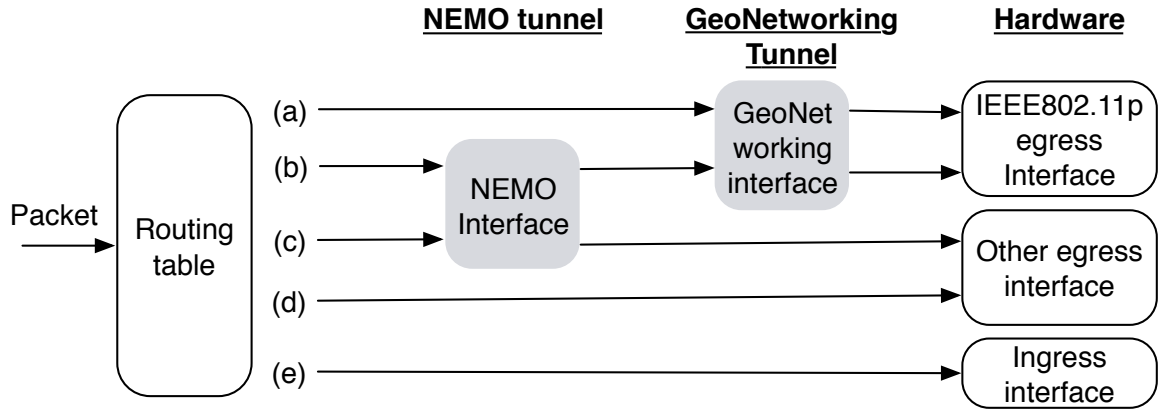


Figure 8.4: Interface management for IPv6 GeoNetworking

must be used when trying to reach other nodes not directly attached to the GeoNetworking link.

The mechanism used to configure the IPv6 GeoNetworking egress interfaces of MRs in an automatic way is based on the IPv6 Stateless address auto-configuration protocol specified in [rfc4862]. This protocol basically enables a host to generate its own addresses using a combination of locally available information (interface identifier part of the address) and information advertised by routers (prefixes that identify the location of the subnet in the Internet topology). The concept used to configure IPv6 addresses over the GeoNetworking link is the same: ARs advertise prefix information by sending Router Advertisements (that can be unsolicited or sent in response to a Router Solicitation), and MRs use that prefix information, together with their GeoNetworking ID, to generate a valid global IPv6 address to be assigned to its GeoNetworking egress interfaces. A link-local address is also generated on the GeoNetworking egress interface, using the same GeoNetworking ID and the link-local IPv6 prefix (fe80::/64).

A prefix length of 64 bits is used and thus the length of the GeoNetworking ID is 64 bits. Consequently, the GeoNetworking ID is used as the GeoNetworking interface identifier. It should be noted that at a given time an MR may have more than one GeoNetworking ID, and therefore may generate more than one different IPv6 address. This can be used to change periodically the IPv6 address used by a node and make privacy attacks harder to perform.

GeoNetworking IDs are assumed to be globally unique at the GeoNetworking. Therefore, the use of the DAD mechanism defined in [rfc4862] is disabled.

8.5 GeoIP SAP

The four GeoNetworking communication types described in Section 3.3.2.2 must be mapped to a corresponding type of communication in the IP layer. We must thus define a module that transfers packets between the IP layer and the GeoNetworking layer and (1) map the IP destination the collect GeoNetworking ID when packets are transferred from IP to GeoNetworking (2) map the GeoNetworking ID to the correct IP destination when the packets are transferred from GeoNetworking to IP. This module comprise an interface (Service Access Point (SAP)) between the two layers.

As shown in Table 8.1, IP unicast is for GeoUnicast. IP multicast is used for GeoBroadcast

and TopoBroadcast. IP anycast is used for GeoAnycast.

Destination	IPv6 layer	GeoNetworking layer
A node in a specific vehicle	IP unicast	GeoUnicast
Nodes in vehicles in a given geographic area	IP multicast	GeoBroadcast
Nodes in vehicles x hops away	IP multicast	TopoBroadcast
A node in a certain vehicle in given area	IP anycast	GeoAnycast

Table 8.1: Relation between destination types at the GeoNetworking and the IP Layer

GeoIPv6.request is defined to transmit the packet from the IP layer to the GeoNetworking layer. As illustrated in Table 8.2, this function provides three parameters: scope, destination and payload.

- **scope**: according to the destination type as described in Table 8.1, four scopes are needed: *GeoUnicast*, *GeoAnycast*, *GeoBroadcast* and *TopoBroadcast*. These correspond to IPv6 unicast, IPv6 anycast, and IPv6 multicast packets, respectively.
- **Destination**: In unicast, IP provides the IP next hop as the destination address and the geographic routing module determines the corresponding GeoNetworking ID from the IP next hop. On the other hand, in the case of GeoBroadcast and GeoAnycast, GeoDestination ID is provided to the GeoNetworking layer. For circle area, the center position (latitude and longitude) and radius is resolved at the GeoNetworking layer from the GeoDestination ID. For TopoBroadcast, the hop limit is provided.
- **Payload**: contains the entire IP packet.

Destination\Parameters	Scope	Destination	payload
A node in a specific vehicle	GeoUnicast	GeoNetworking ID of IP next hop	IPv6 packet
Nodes in vehicles in area	GeoBroadcast	Area ID, Radius	IPv6 packet
Nodes in vehicles x hops away	TopoBroadcast	Hop limit	IPv6 packet
A nodes in certain vehicle in area	GeoAnycast	Area ID, Radius	IPv6 packet

Table 8.2: Parameters of the GeoIPv6.request

For IPv6 unicast / GeoUnicast packets, the destination corresponds to the IP next hop address, not the final destination as shown in figure 8.5. The GeoNetworking layer uses directly this address for multi-hop routing. The IP next hop must first be determined by the IP layer and should then be provided to the GeoNetworking layer.

For IPv6 multicast / TopoBroadcast, only the hop-distance must be transmitted. For IPv6 multicast / GeoBroadcast, the destination (i.e. GeoDestination) corresponds to the coordinates of the geographic area where the packet shall be GeoBroadcast. The actual parameters transmitted by *GeoIPv6.request* depend on the approach adopted to encode the GeoDestination at the IP layer.

For IPv6 anycast / GeoAnycast, the destination (i.e. GeoDestination) corresponds to the coordinates of the geographic area where the packet shall be GeoBroadcast, as for the IPv6 multicast / GeoBroadcast case.

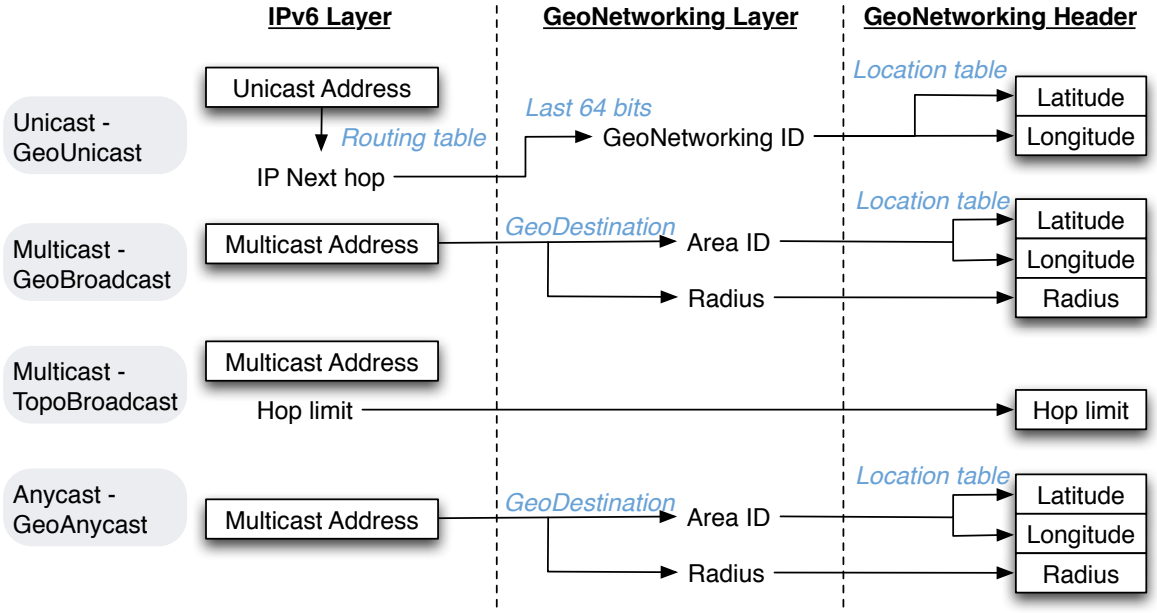


Figure 8.5: SAP for IPv6 over GeoNetworking

8.6 Area based subnet model

Auto-configuration in MANET has a long history of discussion as described in Section 3.3.3. The GeoNet project defined the geographic link as illustrated in Figure 8.6. The GeoNetworking layer plays the role of a sub-IP layer. Thus the access layer (i.e. IEEE 802.11p in the context of the GeoNet project, but possibly another one) is not visible to IPv6. IPv6 packets are sent down to the GeoNetworking layer and encapsulated with a GeoNetworking header. On the IP next hop, the GeoNetworking layer removes the GeoNetworking header and delivers the packet up to the IPv6 stack. Two IPv6 neighbors can be connected by more than one wireless hop, but this is transparent to IPv6 thanks to the GeoNetworking layer.

In the case where a vehicle ITS Station sends packets to the Internet, the IPv6 GeoNetworking link is defined as the broadcast area around the AR in which IPv6 multicast messages are transmitted (such as Router Advertisement, sent to all-nodes multicast IPv6 address). This area is defined by means of a geographic area (Area based subnet model). Thus, an IPv6 GeoNetworking link is composed of all the nodes within a defined geographical area, containing at least one AR. The geographic area can be specified for example, 3 kilometers from the AR. IEEE802.11p is designed to reach up to 1 kilometers, the geographic area is several hops from the edge to the AR.

Different IPv6 prefixes are assigned to an AR in different areas. The on-link/off-link destination determination is based on the comparison of the destination address and the on-link prefix list (or the routing table): if the prefix of the IPv6 destination address is on the on-link prefix list, the destination is assumed to be on-link while the destination is considered to be off-link, otherwise.

By the geographic link definition of GeoNet project, one can assume that every vehicle ITS Station in a geographic link has at least an IPv6 address which is generated from the same prefix. For example in Figure 8.6, the vehicle (a) and the vehicle (b) have an IPv6 address with the same prefix advertised by AR1.The Router Advertisement is delivered until

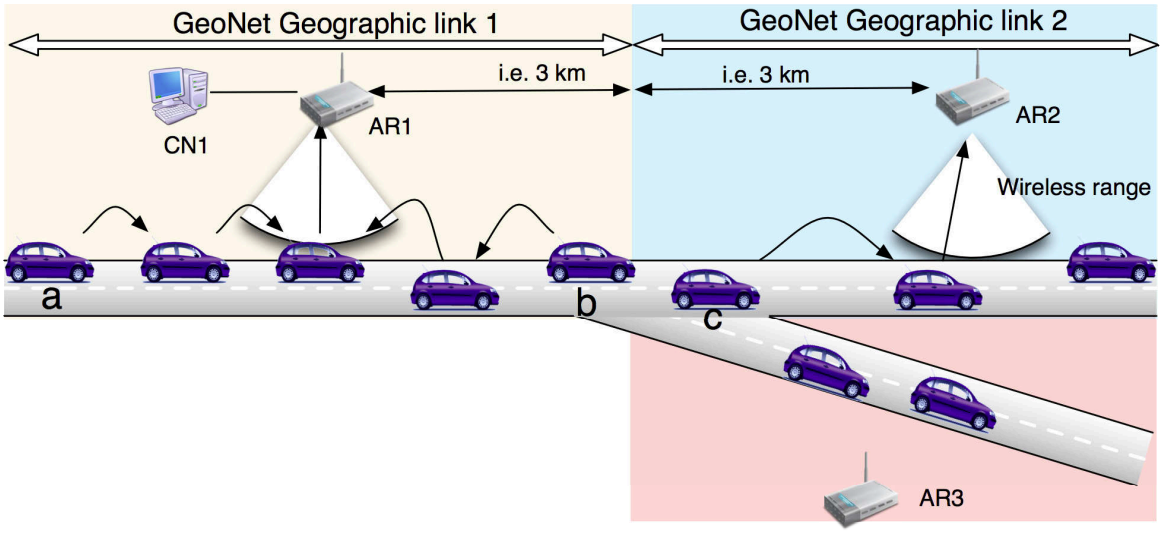


Figure 8.6: Area-based subnet model in GeoNet Project

3 km from AR1 using intermediate nodes as GeoBroadcast relays. The packets from the source addresses that is topologically correct in Geographic link 1 always sent to the AR1.

However this definition is not always desirable, because it causes failure in the edge of the geographic link. For example, the vehicle (b) is at the edge of the geographic link 1 in Figure 8.6. The vehicle ITS Station is going to move to another geographic link. The vehicle movement is predictable. Thus the ITS Station MR should attach to the next candidate AR. Current geographic link definition prevents MR to select the ARs to the Internet. In the case of vehicle (b) in Figure 8.6, it may know the next candidate AR from information contained in LDM, the record of every day's trajectory, or the destination specified in the car navigation system (See Chapter 6.2.2).

In the future, it is important that MR makes a decision for the AR selection based on these kinds of information. Moreover, the MR does not always want to use the next candidate AR, but previous AR. For example, if the vehicle (b) moves to the position of vehicle (c) while the vehicle (b) has a communication flow with CN1 that is connected to AR1, vehicle (b) should keep using the previous IPv6 source address. So it is desirable to select the next and previous ARs at the same time. Hence simultaneous usage of ARs is most favorable.

One more issue of the geographic link definition is the difficulty of AR installation and configuration. Because an AR must exist in a geographic link in the link definition, the AR must be installed and configured in a way not so that it does not overlap with other links managed by other ARs. This limits where ARs could be installed. Roadside ITS Station network administrator may not be able to install ARs to the best place for communication. For instance, building, bridge and base station of 3G are good places to put ARs for VANET, but it is not possible to install them to the place because lack of flexibility of the AR installation.

The rule that a geographic link must comprise an AR is also a restriction for providing performant Internet connectivity. Because road traffic has some points with very high vehicle density e.g. in case of traffic jam. Most of such points, for example, center of city, tollgate, road signal and juncture of roads, are predictable and so, in theory, the network administrator of roadside ITS Stations may be able to install more ARs to prepare for high network traffic. But in practice, it is difficult to put more ARs in certain areas. If the geographic link size is

same in all the area, it is not possible to change AR density. In addition, if the geographic link can be configured with different sizes, the configuration to make the geographic links not overlapped should be complicated, because each AR should be aware of the other ARs and be coordinated with them. In addition to the difficult configuration, the addition of ARs forces to change the configuration of the other ARs.

8.7 End Based Geographic Link Model

To solve the problems of area based subnet model discussed in Section 8.6, we propose a new link model we refer to as End based subnet model. In contrary to the Area based subnet mode, the address is selected by the vehicle ITS Station. The comparison of both models is illustrated in figure 8.7. The proposed model has the advantage that a vehicle ITS Station can select the IP address with more precise vehicle's information such as GPS position, wireless signal strength, the destination of vehicle, digital maps and so on. The end node intelligence makes the address selection more efficient.

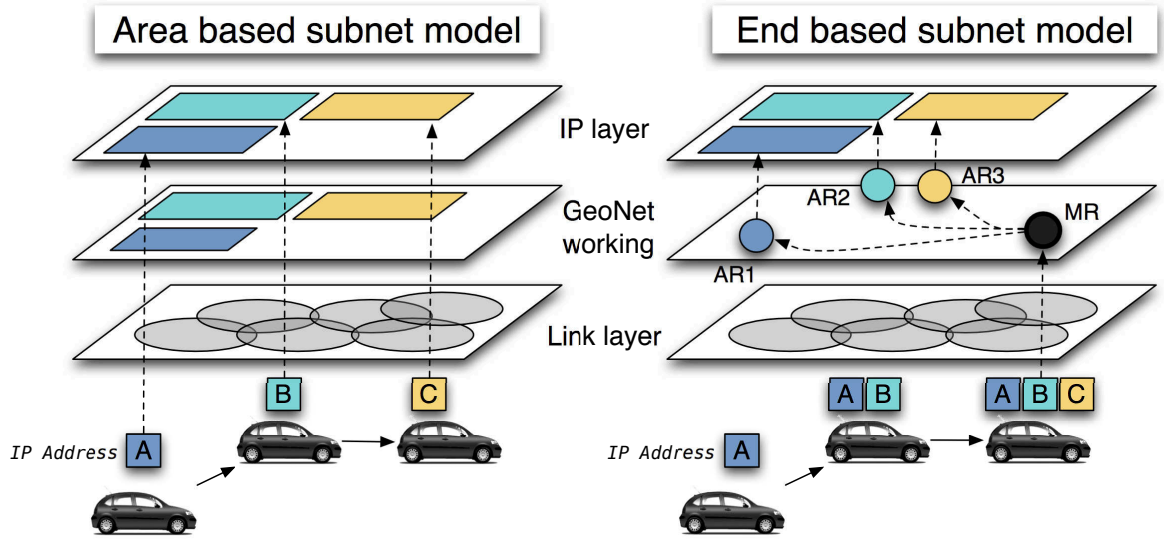


Figure 8.7: Area based link and MR based link

In both models, AR configures the area that the Router Advertisement is transmitted. When an MR receives the Router Advertisement using the area based subnet model, the MR is restricted to use the IP address generated from the Router Advertisement. On the other hand, the proposed model allows the MR to add the address to the candidate list and to select the most preferable IP address in the list at the moment (See Section 6.2.3 for details about path selection). As shown on the righthand of Figure 8.7, the MR accumulates the available IP addresses as the vehicle ITS Station moves.

The MR has its own position information, neighbor vehicle ITS Stations and ARs in the location table with GeoNetworking functionality. MR can calculate that the vehicle is approaching to which AR, and leaving from which AR with relative velocity. From the information, MR can select the gateway AR with own preference. The MR can continue using the same address over the geographic link for existing flows with vehicle ITS Station management decision. Moreover multiple IP addresses can be used for different flows at the same time.

The area based subnet model does not permit to configure multiple IP addresses from different geographic links at the same time. Thus the operator of ARs should avoid the overlapping of the geographic link. It is complicated for the AR operator to configure the distance the Router Advertisement shall be transmitted. In contrary to the area based subnet model, the proposed model allows the overlapping of Router Advertisement area from AR, because the address that MR uses is selected by the MR.

In addition to easiness of configuration, the Router Advertisement area can be configured dynamically in the proposed model. For example, an AR can shorten the Router Advertisement range when the traffic load increases. By reducing the range, less MRs receive the router advertisement and less incoming traffic is received at the AR. In contrary, an AR can configure longer range of Router Advertisement when it has enough capacity of traffic transmission.

Part III

Implementation and Evaluation

Chapter 9

Implementation

Contents

In this chapter, we present the software implementation of our system. All the modules are implemented in the ITS Station router runs the Linux operating system. We introduce Routing Policy Database (RPDB) for IPv6 routing in order to enable the simultaneous usage of multiple paths (*e.g.* vehicle-based, roadside-based and Internet-based), that is one of design requirements described in Chapter 4. Three different GeoNetworking implementations have been developed during this thesis: two of them were implemented under the framework of the GeoNet Project, and the other one was implemented by IMARA(France) and Espritec(Tunisia) collaboration team. We (INRIA) provided a sample code of GeoIP-SAP defined in Chapter 8 to all the implementations and led the validation of the all the implementations. The IPv6 packets are transmitted to the GeoNetworking module via TUN virtual interface. This virtual interface allows IPv6 to treat the GeoNetworking module as one of the Communication Interfaces (CIs) from IPv6 point of view. The path selection manager described in Chapter 6 was partially implemented as an extension of the open-source NEMO implementation (NEPL). The path availability estimation described in Chapter 6 is used to select the appropriate AR.

Implementation of simultaneous usage of multiple paths are published in [Tsukada2008, Tsukada2010a], and the details of the two IPv6 GeoNetworking implementations in the framework of the GeoNet project can be seen in [GeoNet-D.3, Tsukada2010b, Ines2010]. The other IPv6 GeoNetworking implementation is published as an open source CarGeo6 package [Toukabri2011].

9.1 Overview of Implementation

The proposed system is implemented on Linux operating system. Figure 9.1 shows the overview of the implemented system.

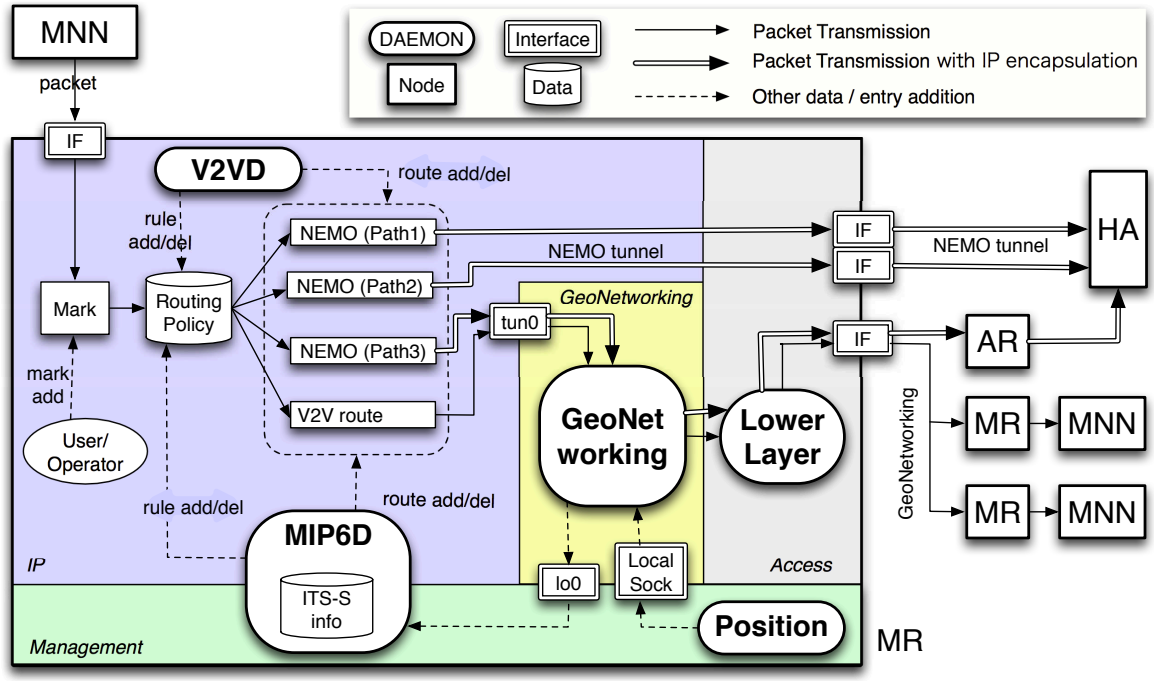


Figure 9.1: Overview of Implementation

There are five modules (daemons) locate in IP, GeoNetworking, Management and Access layers in Figure 9.1. These modules can be replaced by the other implementation. During the thesis, we have developed three versions of GeoNetworking daemons. Two implementations have been implemented with HITACHI and NEC in GeoNet project (See details in Section 2.1.2.1). In the project, HITACHI and NEC implemented the modules independently. The implementations are developed, validated and evaluated in the project. We confirmed that the implementations are fully interoperable each other. The GeoNet implementation is described in Section 9.3.1. The other implementation called CarGeo6 is developed by IMARA(France) and Espritec(Tunisia) collaboration team. The implementation is open source software not like as the GeoNet one. The implementation has a form that the GeoNetworking modules and LowerLayer module are merged into one united module. Thus GeoNetworking functionality is actually realized with two modules (GeoNetworking module and Position sensor module.) The CarGeo6 implementation is described in Section 9.3.2. INRIA has contributed implementation of GeoIP SAP part (see details in Section 8.5) for all the implementations.

The V2V daemon (V2VD) also has two varieties that are OLSR daemon and MNPP daemon. V2VD is running in the IP layer that maintain the V2V direct path between vehicles. In the IP layer, NEMO daemon (MIP6D) operates NEMO and MCoA. MIP6D and V2VD are cooperating each other to enable both of the NEMO path and the V2V path simultaneously. The implementation of Simultaneous usage of NEMO and V2V is detailed in Section 9.2.

The packet comes from the IP layer is directed either directly to the egress interface or to GeoNetworking layer. The packet goes to GeoNetworking layer is sent to GeoIP SAP that is implemented as a virtual interface of tun0 in the system. GeoNetworking modules receives IP packet from tun0 and encapsulates it with GeoNetworking header. GeoNetworking functionality is realized with three modules that are GeoNetworking module, LowerLayer module and Position sensor module.

To enable Address selection in End Based Geographic Link Model, the MIP6D is extended. The AR list database and Address Selection function in the Management layer is actually implemented in MIP6D, because currently all the database and function is used in MIP6D. When GeoNetworking module receives RA from AR, the position information is sent to MN-SAP that is implemented as local raw socket (lo0). MIP6D receives the AR position information and decide Access Selection according to the information. The MN-SAP enabled MIP6D that works with CarGeo6 is described in Section 9.4.

9.2 Simultaneous usage of NEMO and V2V

9.2.1 Policy routing

A policy routing algorithm has been developed and integrated in the architecture to allow simultaneous usage of NEMO path and V2V path. This subsystem allows vehicles to communicate with each other over both the fixed and VANET networks at the same time.

To distribute packets to multiple paths simultaneously from a MR, a policy routing scheme has been designed. Classic routing mechanisms are not suitable because of the "*longest match*" principle. As shown in Figure 9.2, packets arriving to the MR are forwarded to the routing table entry which has the longest prefix in common with the destination address. In the simultaneous usage of NEMO and V2V case, V2V paths typically have longer prefix lengths than NEMO ones. The formers are thus used in priority when they are available in the routing table. NEMO paths then have the least preference and are used as default paths. A

single routing table can be used for switching between paths but not for simultaneous usage of NEMO and V2V.

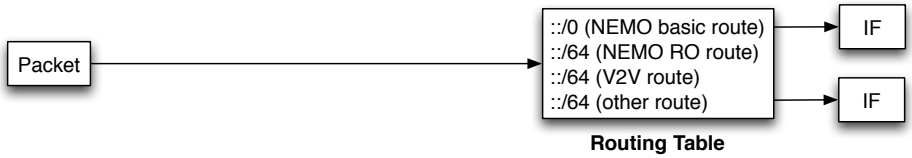


Figure 9.2: Classic routing

To solve the previous problem, we propose multiple routing tables using a RPDB, as shown in Figure 9.3. To achieve this goal, the Netfilter[1] framework is used. The RPDB allows to maintain several independent routing tables in the kernel. Each packet can then be routed according to any of these tables. The determination of which routing table that should be used in a particular case is up to the implementation. It is usual to route depending on the type of flow that is being treated. This mechanism allows distributing packets to multiple concurrent routes at the same time.

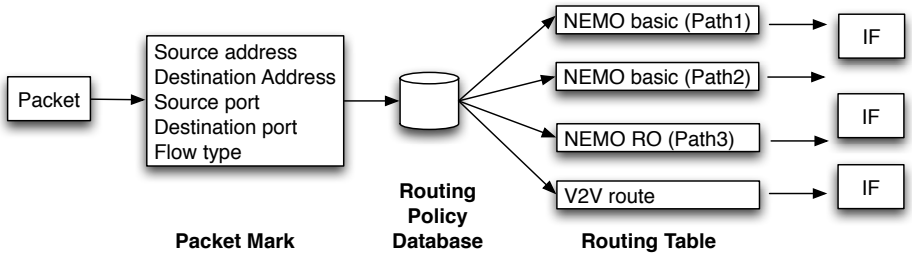


Figure 9.3: Multiple Routing Tables

9.2.2 Implementation Details

NEMO Platform for Linux (NEPL) has been installed on MRs along with the daemon that takes care of V2V route (MNPP, OLSR and etc.) NEPL is developed and distributed freely by Nautilus6[2] within the WIDE Project[3]. NEPL is based on Mobile IPv6 for Linux (MIPL)[4], developed by the Go-Core (Helsinki University of Technology) and Nautilus6 projects.

The V2V daemon has been adapted to the routing scheme proposed in Section 9.2.1. In this way, V2V routing entries are maintained in one of the multiple routing tables of the kernel. The NEMO daemon already handles policy routing when patched for MCoA Support[5].

NEMO and V2V daemons operate independently in MRs. The NEMO one maintains its binding update list and NEMO paths, while the V2V daemon takes care of V2V paths. As shown in Figure 9.5, both NEMO and V2V routing entries are kept up-to-date in separate tables.

[1] http://www.netfilter.org
[2] http://www.nautilus6.org
[3] http://www.wide.ad.jp
[4] http://www.mobile-ipv6.org
[5] http://software.nautilus6.org/MCoA/

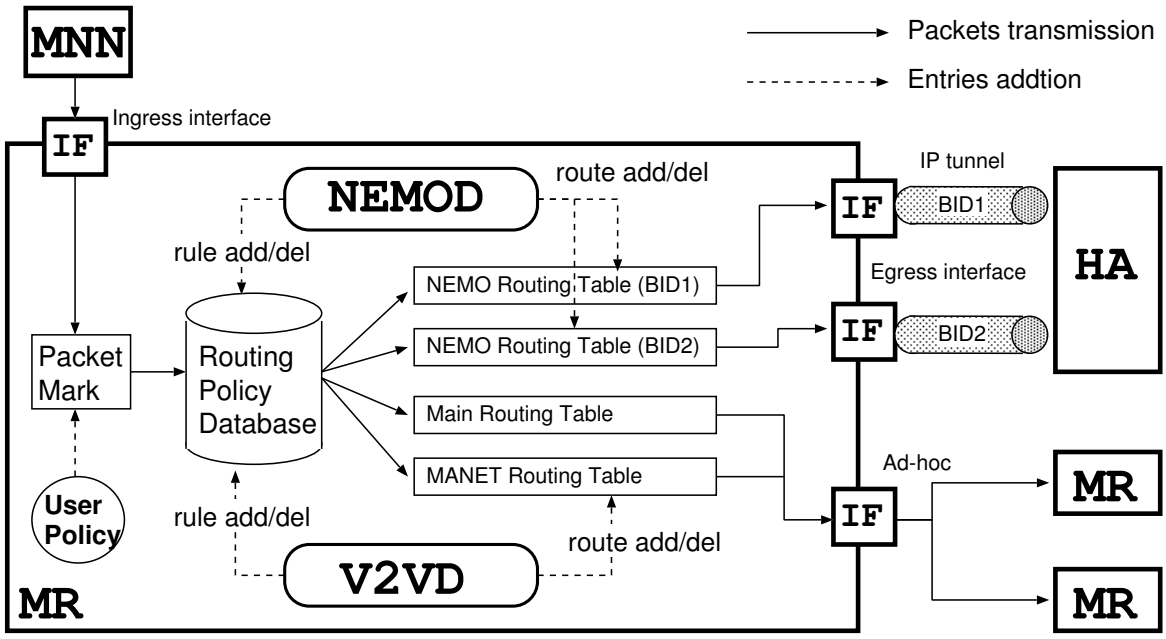


Figure 9.4: Implementation detail of Simultaneous usage of NEMO and V2V

When started, both daemons add rule entries that specify which packets should be routed according to which routing table (these are removed at the execution end). MRs have multiple routing tables, which save NEMO and V2V paths, and the default one (depicted as MAIN in Figure 9.5), which saves the rest of paths. There is the same number of NEMO routing tables as egress interfaces on the MR. Each of these routing tables has a specific BID. The V2V routing table is used for traffic that should be routed directly to neighboring vehicles, and the MAIN table is mostly used to route signaling message.

Packets from MNNs arrive at the MR containing the source and destination addresses and ports, as well as the flow type information. Packets are distributed according to the latter mark to either the NEMO or V2V routing tables. Packets matched with a NEMO routing table are transmitted to the tunnel bound to the HA, while packets matched with the V2V table are transferred to other vehicles directly.

9.3 Geographic routing implementation

9.3.1 GeoNet Implementation

The prototype system is implemented on GNU/Linux (kernel 2.6.29). In this section, design and implementation are mentioned. The GeoNet project has produced two independent implementations of GeoNetworking layer (HITACHI implementation and NEC implementation), and one of the IPv6 over GeoNetworking module and the GeoIP SAP (previously called C2C-IP SAP, see details in Section 8.5). GeoNetworking developers implemented it independently without seeing the source code each other from same GeoNet specification. The interoperability between the two proves that there is a common and correct understanding of the specification. Both implementations of the GeoNetworking layer have been utilized in the experimental performance evaluation in Chapter 10.

The GeoNetworking functions are divided into three main modules that cooperate each

other. The three modules are implemented in userland for ease of implementation and modification. Remind that one of objective of the project is to brush the specification up by feedback from the implementation. The three modules are responsible of particular function on MR. These modules cooperate via inter-process communication socket. **PositionSenser** module is to create a stable interface for acquiring geographic data by the GeoNetworking modules. It is implemented as a stand-alone program connected to a positioning service available for a particular platform. It sends the position information over a UDP socket to GeoNetworking modules. **LowerLayer** module is the interface between GeoNetworking (GeoNet internal modules) and the PHY/MAC Layer. This is needed to support the platform independency of GeoNet. It allows GeoNet to support different platforms with different network interfaces without holding platform specific parameters within the GeoNetworking modules. **GeoNetworking** module controls the position information and keeps transmitting a periodic packet to inform its neighbors about its presence. It also transmits received data with GeoNetworking header to LowerLayer module via UDP socket. GeoIP SAP, which has *GeoIPv6.request* function described in Section 8.5, is integrated into GeoNetworking module.

In Linux system, IPv6 packet forwarding is processed in the kernel space. However the packet has to be brought to the user land from kernel, because the GeoNetworking module is implemented in userland. Then the packet is encapsulated with GeoNetworking header and then sent back to the kernel again. We decide to use TUN virtual interface to bring the packet to the user land. Overall process of IPv6 over GeoNetworking is illustrated in Figure 9.5.

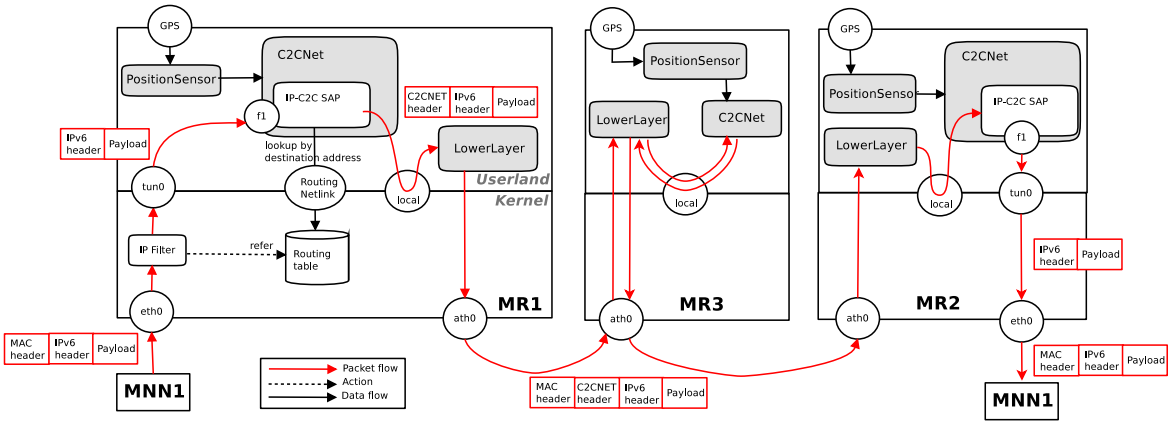


Figure 9.5: Implementation Overview of IPv6 over GeoNetworking

MNN1 sends IPv6 packets to MR1 that is the default router of in-vehicle network. MR1 receives the packets on the ingress interface (eth0 in Figure 9.5) and removes MAC header of the packets. Then IP header and payload part are transmitted into the tun0 virtual interface by the pre-configured rules of IP Filter[6]. The GeoNetworking module reads the data from tun0 and parses the information of the IP header.

The destination IPv6 address is used to distinguish communication type whether unicast or multicast by the first 8 bits which are correspondent to GeoUnicast and GeoBroadcast, respectively.

In multicast case (first 8 bits are filled by 1 (*0xff*)), destination GeoNetworking information are pre-configured depending on the destination IPv6 address (i.e. if the destination

[6] http://www.netfilter.org

address is link-local all node multicast address (ff02::1), the latitude and longitude are as well as those of MR1 and the radius is 500 meter).

In unicast case (first 8 bits are not filled by 1 (*0xff*)), the next hop IPv6 address is resolved from the routing table via *netlink* library by the destination IPv6 address. The last 64-bits of the next hop IPv6 address is correspondent to the destination GeoNetworking ID. The module can add the ID into the GeoNetworking header. The latitude and the longitude of the destination can be resolved using the ID from the location table maintained in GeoNetworking module. The latitude and the longitude are also put in the GeoNetworking header.

The data with GeoNetworking header, IPv6 header and payload are sent to LowerLayer module via local UDP socket. LowerLayer module adds MAC header over GeoNetworking header and transmits the frame into the air. The intermediate node (MR3) receives the frame and re-transmits the frame when GeoNetworking modules find that the frame should be re-transmitted to reach the destination with multi hop manner.

Finally, MR2 receives the frame and on the egress interface. Then LowerLayer module removes the MAC header. The GeoNetworking module finds that the destination of the GeoNetworking packet is MR2. The IPv6 header and payload are sent to the tun0 virtual interface. The packet is routed to egress interface (eth0). MNN2 receives the IPv6 packet that sent from MNN1.

9.3.2 CarGeo6 Implementation and GeoNetworking-aware MIP6D

CarGeo6 is an open source implementation of CALM/ETSI compliant geographic routing module. Since GeoNet also follows CALM/ETSI specification, the concept is almost same. Thus description about IPv6 over GeoNetworking in Section 9.3.1 is common with CarGeo6. A little difference is that CarGeo6 includes LowerLayer functionality that is separate modules in GeoNet implementation.

GeoNetworking-aware MIP6D is an extension of MIP6D so that the MR generates and configures an IP address from GeoNetworking ID that is specified at start up from the configuration file. GeoNetworking-aware MIP6D generates CoA from the RA prefix as a network ID (first 64 bits) and GeoNetworking ID as a host ID (last 64 bits).

In this section, we describe about the signaling and packet flow of NEMO with CarGeo6 using Figure 9.6. MR and AR have same functionality in CarGeo6, and the difference is that GeoNetworking-aware MIP6D is installed in MR and RADVD is installed in AR. As Figure 9.6 shows, CarGeo6 have four interfaces including two network interfaces (tun0 which is virtual interface between IP and CarGeo6 and ath0 that is wireless interface) and routing socket to the routing table and Unix socket to GPS sensor. Beside IP over GeoNetworking function, the main functions in the CarGeo6 are categorized by four kinds function that are

1. **Beaconing**
   Periodic exchange of location information to GeoNetworking neighborhood. It is broadcast message from a GeoNetworking interface to all the node connected with single hop to a source node. Beacons must not forwarded in basic specification.

2. **Sending** (GeoUnicast and GeoBroadcast)
   IP unicast is translated in GeoNetworking layer to GeoUnicast that is sent to a specific location. IP multicast is translated in GeoNetworking layer to GeoBroadcast that is sent to a specific area.

3. **Receiving** (Receive and forward)
   Reception of GeoNetworking packet and calculation of forwarding. When the node that receives the packet is the destination, it sends the packet to IP over GeoNetworking function. If not, it calculates the next hop neighbor with the current location and the destination location. If it cannot find any neighbor, it stores the packet certain time of period until finding neighbor to forward.

4. **Location service**
   Resolution of destination GeoNetworking node's location by flooding the solicitation of location and answer from the destination node.

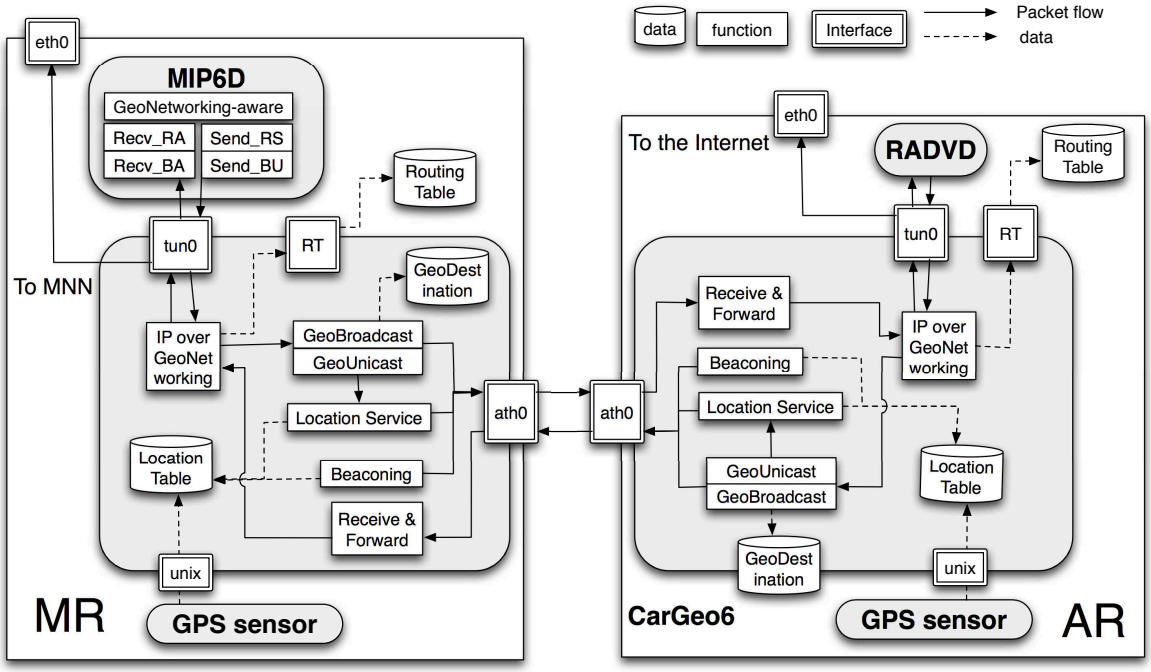


Figure 9.6: Implementation overview of CarGeo6

MR and AR are exchanging beacons to the neighbors and updating the neighbors' position information in the location table. The position of own node is also regularly obtained from GPS sensor via Unix socket and registered in the location table.

The MIP6D sends a RS to find an AR by RA (*Send_RS*). The RS is sent from MIP6D to tun0 and is received by IP over GeoNetworking in CarGeo6. The destination address of RS is all-router-multicast address (ff02::2), thus IP over GeoNetworking function finds that the packet uses multicast over GeoBroadcast from the first 8 bits (0xff) of the destination address just as described in Section 9.3.1. The GeoBroadcast function translates the destination address to the location information (latitude, longitude and altitude) by GeoDestination database that is statically configured at the startup. GeoBroadcast encapsulates the IP packet with GeoNetworking header that has the location information.

The packet sent from ath0 of the MR, may be forwarded by multiple hop manner until the border of the destination area. If an AR is inside of the area, the function of *Receive* in AR's CarGeo6 receives packets and sends it to IP over GeoNetworking function. IP over GeoNetworking simply decapsulates the GeoNetworking header and write the inside IP packet

to the tun0 interface. From RADVD side, it is configured to monitoring all router multicast packet in the tun0 interface.

When RS message from MR is written in tun0 from CarGeo6 of the AR, the RADVD reacts to send RA to all node multicast (ff02::1) on tun0 interface. RADVD also sends RA periodically even if there is no router solicitation. The RA is delivered to the MR if the MR is still in the destination area of the RA.

When the RA is written in tun0 of MR, MIP6D configures CoA on tun0 according to the network prefix in the RA and GeoNetworking ID specified in the configuration file. At the same time, the default route is set to the tun0 address of AR from source address of the RA. Then, the CoA is sent by BU from the MR to the HA. The BU is sent to the tun0 and IP over GeoNetworking receives the BU. This time, GeoUnicast is taken as communication type in GeoNetworking layer, because the destination address of the BU is unicast address (HA address). The destination GeoNetworking is resolved by looking the routing table up with routing socket. Because HA is located in the Internet, the default route should be selected as IP next hop that is AR's tun0 address for BU's case. The last 64 bits of the default route is AR's GeoNetworking address, because AR's tun0 is configured with GeoNetworking ID. By GeoNetworking ID, MR may be able to find the AR's position in the location table, if they exchange beacons or the entry of AR's position that has been taken by the last location service, and it has not been expired. If it does not find AR's position, MR send location service message to the network until AR replying its position. The AR's position in reply message of AR is used for GeoUnicast packet header and also registered in the location table.

The BU message is delivered to the AR and received on the AR's position. Since the destination GeoNetworking ID of the GeoUnicast packet is AR, *Receive and forward* function sends the packet to IP over GeoNetworking function. GeoNetworking header is removed and inside IP packet is written to tun0 interface. The destination of the IP packet (BU) is the HA, thus the packet is delivered to the HA by normal IP routing. The HA replies a BA to the CoA as usual NEMO signaling.

BA arrives to the AR and transferred to MR by unicast using GeoUnicast, because the destination address of BA is an unicast address (CoA). Upon receiving the BA by MIP6D, the MR create NEMO tunnel to the HA. NEMO tunnel is recognized by *ip6tnl* in Linux system and the MR may have several *ip6tnl* interfaces for MCoA support.

The packet from MNNs behind the MR is delivered to the HA via NEMO tunnel. It is first sent to *ip6tnl* and encapsulated by IP header with NEMO. Then the encapsulated packet is received by IP over GeoNetworking via tun0. If the next hop device is *ip6tnl* when IP over GeoNetworking resolves the next hop, the default route is taken as a next hop because the destination of outer IP header is the HA. Encapsulated packet is delivered to AR by GeoUnicast. The AR processes the packet as usual GeoUnicast packet and routes it to the HA by normal IP routing.

9.4 Implementation of MIP6D and CarGeo6 Interaction

MIP6D and CarGeo6 interaction is implemented as extension of both daemons. NEPL version 0.4 patch and MCoA patch are applied to MIP6D. The MIP6D also has GeoNetworking-aware functionality described in Section 9.3.2. CarGeo6 version 0.9.8 is used.

Figure 9.7 shows the overview of the interaction between MIP6D and CarGeo6. White boxes are the function that original daemons had and the colored boxes are the functions that are newly implemented. To enable the new functions, the user specifies $-m$ option in start up of the both MIP6D and CarGeo6.

The functions in MIP6D and CarGeo6 locate in three layers of IP, GeoNetworking and Management, as the figure illustrates the in the three layers. The new functions converged in adaptation entities (in both daemons) and management entity (in MIP6D). The management entity are not implemented as an independent program but integrated in MIP6D. This is because MIP6D is the only one module that receives the decision from the management entity at this moment.

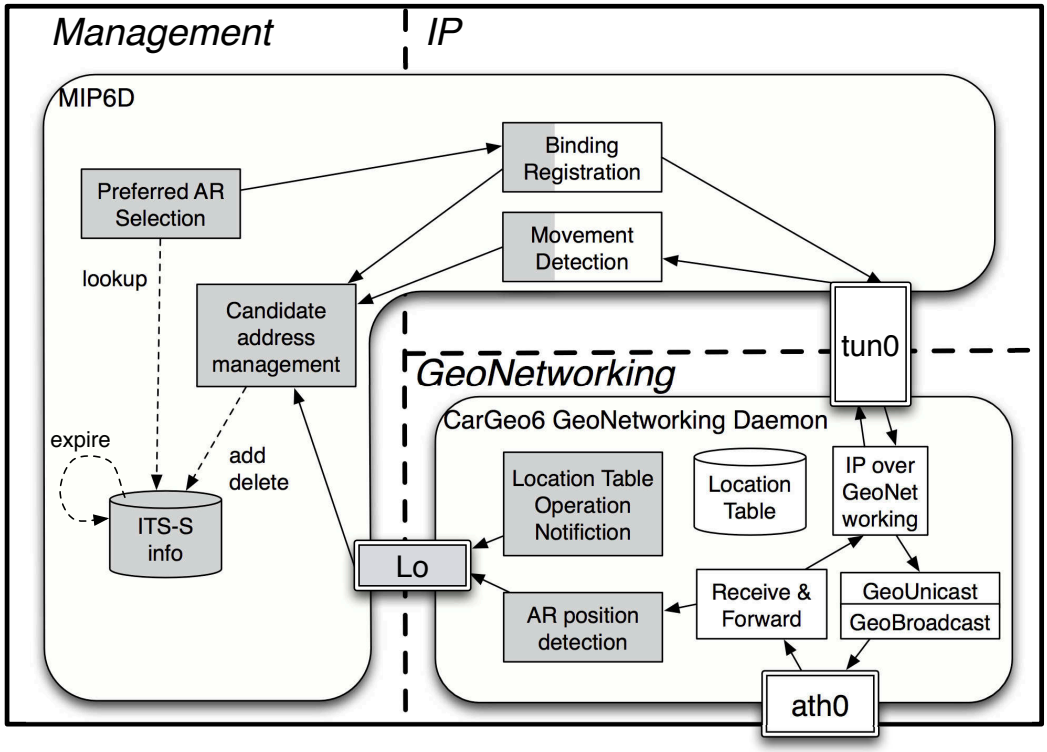


Figure 9.7: Overview of MIP6D implementation with MN-SAP

The functions illustrated with white boxes work as described in Section 9.3.2. The difference is that CarGeo6 sends the AR position information to the management entity via local UDP socket (corresponding to *STAGeoNot.request*), when it receives a RA. CarGeo6 takes the geographic information of the AR from the common header of the RA brought by GeoBroadcast. The message sent to the management entity from CarGeo6 GeoNetworking daemon includes GeoNetworking ID, latitude, longitude, altitude, speed, heading, accuracy, time stamp and lifetime (See format and details also in Table 7.7). The parameters are comes from the common header of GeoNetworking header except for lifetime. The lifetime comes from the configuration at start up. When the entry of the location table is removed in GeoNetworking daemon, the message of *STAGeoNot.request* is sent to the management entity with only GeoNetworking ID and the lifetime set to zero via the local UDP socket.

In MIP6D side, the *STAGeoNot.request* is received at the candidate address management module. When the message is notification of a location table entry addition, the candidate address management module adds an entry according to the message via MN-SAP. The added ITS Station information table entry is removed when the lifetime expires. When the module receives the notification of ITS Station information table entry deletion, the module removes the corresponding entry of the ITS Station information table as well. By this way,

the ITS Station information table is kept up-to-date.

On the other hand, movement detection modules detect movement on the reception of RA. The module adds network prefix information to the corresponding entry in the ITS Station information table. The corresponding entry is found by looking the GeoNetworking ID by last 64-bits of source address of the RA.

The RA also triggers the Binding Registration. Normal MIP6D sends a BU with the CoA generated from the received RA, however the extended MIP6D sends a BU with the CoA generated from the RA from preferred AR based on decision with the ITS Station information table. The Preferred AR Selection is performed by simplified version of Path Availability Estimation described in Section 6.2.2, when there are more than one ARs recorded in ITS Station information table.

Chapter 10

Evaluation Goals and Methodology

Contents

In this chapter, we present our goals of the evaluation used for the performance evaluation presented in Chapter 11, 12 and 13.

The first section describes the four major goals and the second section presents the methodology using an indoor test environment and an outdoor field test environment mad up to four vehicles. Details of the tests performed are presented in the following section.

The goals are to measure performance improvement thanks to simultaneous usage of multiple paths, the overhead using IPv6 GeoNetworking, the overhead using NEMO over IPv6 GeoNetworking and to analyze various affects of the conditions to the metrics. Then the network configuration, the vehicular platform, parameters, metrics (Round-Trip Time (RTT), throughput, jitter, Packet Delivery Ratio (PDR), the number of hops) and experiment scenarios are described. We developed the packet analysis and visualization tool called AnaVANET in order to understand the affect of various condition to the metrics for outdoor test evaluation.

10.1 Evaluation Goals

The goals of the evaluation are as follows:

- To measure how much network performance improvement is achieved by simultaneous usage of multiple paths in terms of latency and throughput. The measurements are performed both in confined conditions in order to get performance without any unexpected influence and in the realistic conditions and scenarios using vehicles.
- To measure the overhead of an IPv6 GeoNetworking compared against a pure IPv6 stack in terms of latency and throughput. The obtained overhead can be taken into account for the metric of path selection process. As a benchmark, the network performance of a VANET maintained by a standard MANET protocol (OLSR) is measured under the same conditions as the IPv6 GeoNetworking measurements.
- To measure the overhead of NEMO over IPv6 GeoNetworking compared against a pure IPv6 GeoNetworking in terms of latency and throughput. The obtained overhead can be taken into account as a metric for the path selection process.
- To analyze which conditions (*e.g.* distance, movement, obstacle, number of hops) affect which performance metric (*e.g.* packet loss, throughput, delay, etc.). We can catch the tendency of the impact by repeating same scenarios with all the implementations under evaluation. The impact can be checked by *AnaVANET,* a newly developed analysis and visualization tool.

10.2 Evaluation Methodology

To evaluate the performance of the implementations, we make a vehicular network testbed with up to four prototype vehicles (See Figure. 10.1).

All evaluation parameters and evaluation metrics are summarized in Table 10.1.

There are three kinds of implementations that we evaluate (OLSR, GeoNet and CarGeo6). OLSR is the standard MANET protocol that gives us the useful network performance result

Figure 10.1: Prototype vehicles used in the field experiments

used as a benchmark. We uses OLSR because it is a proactive MANET protocol particularly suitable for VANET because we do not need to care about the battery life for periodical signaling and it can sustain highly dynamic network topologies.

Two GeoNet implementations of GeoNetworking were provided by HITACHI and NEC in the GeoNet project. We, INRIA, implemented the adaptation module allowing to transmit IPv6 packets over GeoNetworking through GeoIP SAP previously called C2C-IP SAP.

Both implementation of GeoNetworking follow the GeoNet specification and we verified that they are fully interoperable. The evaluation is performed with each implementation. These implementations run on the LaRA testbed Version 2. The adaptation module that we implemented was integrated into the GeoNetworking sub-layer implementation developed by Espritec after the completion of the GeoNet project as described in Section 9.3.2. The stack combining IPv6 and GeoNetworking was released as CarGeo6.

We evaluate all of these implementations in identical environments (Network configuration, vehicles, location , test scenarios, GPS and antenna). However, some measurements are performed by different hardware platforms in MRs, because our testbed evolved during this dissertation. There are two versions of MR hardware platform and operating system during the dissertation. The first version has the *Soekris* hardware platform and Linux kernel version 2.6.22 with Voyage distribution. On the other hand, the second version uses *Alix* board hardware platform and Linux kernel version 2.6.29 with Ubuntu distribution. Version 1 is used for the evaluation with NEMO and OLSR that described in Chapter 11. Version 2 is used for rest of the evaluations. About network configuration and the detailed equipments used in the two versions are summarized in Section 10.3.

The three implementations are evaluated first indoor in confined conditions and then outdoor in real conditions.

The **indoor test environment** is designed to evaluate the pure performance of IPv6 GeoNetworking avoiding interferences due to unexpected radio perturbations and difficulties to trace the movements of the MRs. The tests are actually performed on a table without any vehicle as shown on Figure 10.2. The GPS information used in GeoNet and CarGeo6 stacks is not from an actual GPS device but from a static position recorded in a configuration file. The advantage of this method is that the same test scenarios can be repeated several times with various parameters.

To evaluate the performance in more realistic scenarios, we setup an **outdoor field test environment** with four vehicles equipped with an MR, an MNN, GPS receiver and wifi antenna as shown on Figure 10.3. The topology of the network dynamically changes during

Conditions	Elements					
VANET protocol	OLSR	GeoNet (HITACHI & NEC)				CarGeo6
Testbed	Version1	Version2				
Test environment	indoor		Outdoor			
& Scenarios	Single hop	Multi hop	Distance	Static	Urban	Highway
Parameters	UDP		TCP		ICMPv6	
	packet size, sending bandwidth		TCP window size, Max segment size		Packet size, send interval	
Evaluation metric	Packet delivery ratio, throughput, Jitter, Hop count		Throughput		RTT, Packet delivery ratio, Hop count	

Table 10.1: Evaluation Parameters and Evaluation metrics

the test depending on the location of the vehicles. The performance of the implementations depends on the radio propagation which is influenced by obstacles. Network performance also depends on other factors such as the distance, movement of vehicles. We have therefore developed the AnaVANET evaluation tool (described in Section 10.8) to perform the evaluation taking into account all of these factors.

Figure 10.2: Indoor Testbed

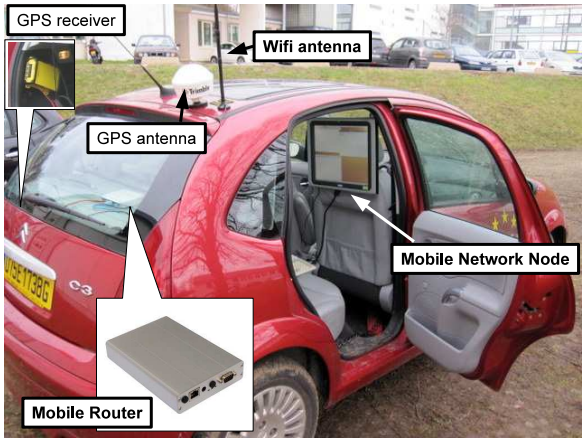


Figure 10.3: Outdoor Testbed

10.3 Evaluation Platform

10.3.1 Outdoor testbed

The testbed comprises a combination of vehicles and roadside as in Figure 10.4. Each vehicle is equipped with a MR, with at least two interfaces: an Ethernet link and an 802.11b adapter in ad hoc mode. MNNs connect to the in-vehicle network via their Ethernet interface (an internal managed Wi-Fi network could also be used for this purpose), while the ad hoc Wi-Fi interface is used for the inter-vehicle connections.

In Figure 10.4, *MR1* and *MR2* are also connected to an infrastructure network using the same 802.11 interface configured in adhoc mode. Whether AR and MR use the GeoNet stack or the CarGeo6 stack, there is no functional difference at the GeoNetworking layer. Both AR and MR also uses Wi-Fi adhoc mode.

On the other hand, when MR connects to the access point in the infrastructure, it should use another 802.11 interface in managed mode. This is because adhoc mode and managed mode are not compatible and it is not possible to both modes at the same time in a single Wi-Fi interface. We use two Wi-Fi interfaces in adhoc and in managed mode on MR to connect to the infrastructure access point we used the testbed deployed by IRISA in the context of the ANEMONE Project (Chapter 11).

MR1 has an additional 3G modem to establish a second link to the Internet (Point-to-Point Protocol (PPP) link provided by SFR[1]). *MR1* is supported by *HA1* at INRIA Rocquencourt and *MR2* is supported by *HA2* inside IRISA's network. Both networks are located in France and interconnected via *Renater*[2] using a direct 6in4 tunnel to work around some IPv6 firewalling problems (the testbed sites are 12 IPv4 hops apart).

10.3.2 LaRA testbed Version 1

Up to four Citroën C3 cars equipped with the proper hardware to create a VANET and log positioning and network traffic information. The MR installed in each car is a *Soekris net4521*, with a mini-PCI 802.11 *Texas Instruments ACX 111 802.11 b/g wireless transceiver* and a compact flash hard disk. The wireless interface has been set- up at 11 Mbps, emulating an 802.11b device. The computer is connected to a *Trimble AgGPS 323* GPS receiver via serial port, whose external antenna is visible on the photo. The wireless card uses another external antenna, fixed on the car's roof too. One of the two ethernet connections of the MR is used to connect it with the in-vehicle wired network, by means of a hub. In the sender and receiver vehicles, a laptop is connected to the in-vehicle network. The sender laptop is a *Windows XP*-based system, whereas the second one comprises a Linux *Debian* computer. A Linux *Voyage* distribution with kernel 2.6.22 has been installed on MRs, and the *olsr.org* daemon 0.5.6-rc7 [3] (an implementation of the OLSR protocol) has been configured on each one.

10.3.3 LaRA testbed Version 2

MRs are *Alix3d3* embedded boxes on which *Ubuntu* 9.0.4 is installed with a Linux 2.6.29.6 kernel. Each MR has one built-in Ethernet port (ingress interface) which is connected to the Ethernet hub connecting other hosts, and a mini-pci wireless card (*Atheros AR5414 802.11*

[1] SFR is a french mobile telephony operator
[2] French backbone for education and research
[3] http://www.olsr.org/

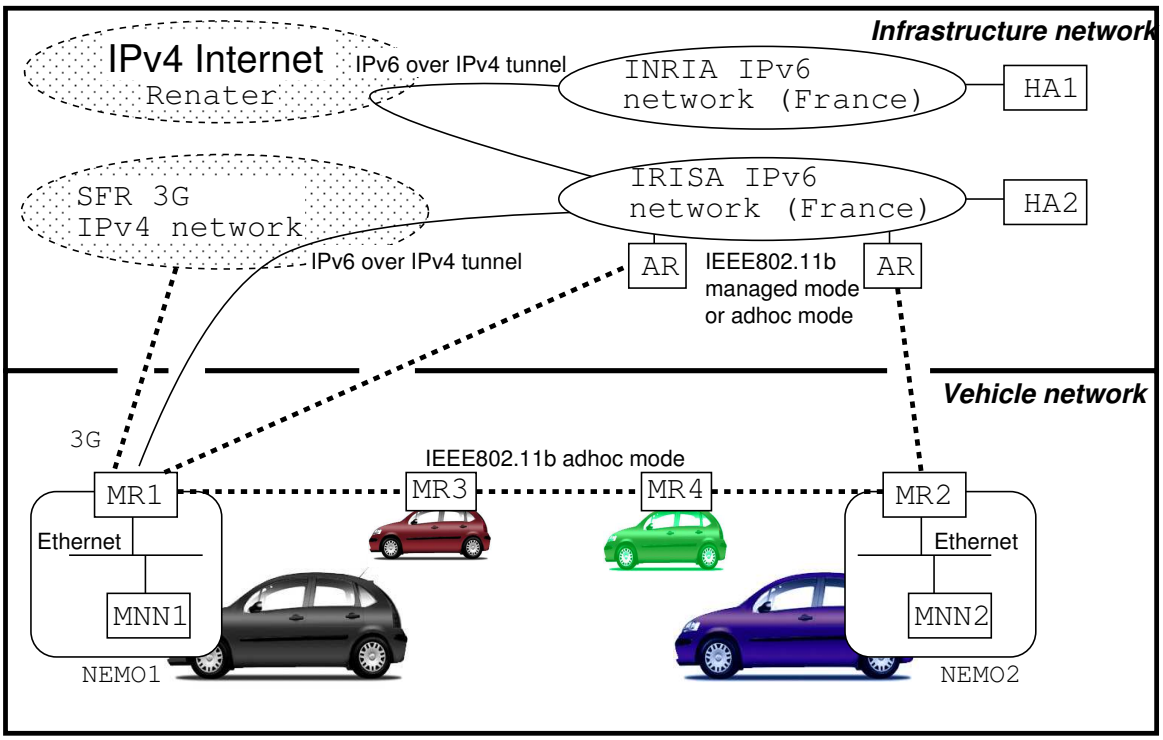


Figure 10.4: Topology of the vehicular network and Internet connectivity

a/b/g Rev 01) used as wireless connection to other MRs. MRs are running the complete IPv6 suite of protocols and the GeoNetworking sub-layer which implementations are presented in Section 3.3.2.2 and implemented in Section 9.3.1 and Section 9.3.2.

MNNs are conventional IPv6 hosts (desktop or laptop) configured with *Ubuntu* 9.0.4. They are connected to the MR through the Ethernet hub. The configuration of MR and MNN is summarized in Table 10.2.

	Model	CPU	Memory	OS
MR	Alix3d3	AMD PCSi586 CPU 498.128 MHz	256MB	Ubuntu 9.0.4, kernel 2.6.29.6
MNN	PAC-1000GB-R20	Intel ® Core(TM)2 Quad CPU Q9650 CPU 2003 MHz	3GB	54-Ubuntu , kernel 2.6.31-17

Table 10.2: Configuration of Nodes (Testbed version 2)

Between vehicles, MRs are connected with IEEE802.11g. The *Madwifi* driver[4] is used for the wireless configuration. The wireless network is configured as follows:

- **Wireless channel**: 3
- **Frequency**: 2.422 GHZ
- **Data rate**: 6 Mbits/s

[4] http://snapshots.madwifi-project.org/madwifi-trunk/

2.4GHz 5.5dBi indoor *EZ-Xtender OMNI RP-SMA*[5] is designed to provide an extended radio coverage. On the other hand, 2.4GHz 9dBi indoor *OMNI antenna RP-SMA*[6] is used for outdoor tests.

This testbed is used to evaluate the performance of the IPv6 GeoNetworking stack for all variants of GeoNetworking (HITACHI, NEC and Espritec) (See Section 10.2).

10.4 Evaluation Parameters

10.4.1 Number of Hops

The performance depends on the network configuration, particularly the number of hops that packets are transmitted through between their source and destination. Thus we can get the best network performance when the MRs are directly connected (single hop). In contrast, multi-hop configuration adds transmission delay and processing delay. The evaluation considers both single hop and multi-hop cases.

10.4.2 Types of communication flows

UDP, TCP and Internet Control Message Protocol version 6 (ICMPv6) are used to measure the network performance between two communication end-nodes (MNN to MNN):

UDP is a connection-less unidirectional transmission flow. The traffic is generated by *iperf*. The tool can configure the sending packet size and the sending rate. Metrics under consideration are Packet Delivery Ratio (PDR), throughput and jitter.

TCP is a connection based bidirectional transmission flow. The traffic is also generated by *iperf*. The tool can configure the TCP window size and maximum segment size. The metric under consideration is the throughput.

ICMPv6 is a bi-directional transmission flow. The traffic is generated by *ping6*. The tool can configure the packet size and the sending interval. Metrics under consideration are the RTT and PDR.

10.5 Evaluation Metrics

10.5.1 Round Trip Time (RTT)

The Round-Trip Time (RTT) is measured using ICMPv6. A host on the source vehicle sends the ICMPv6 echo request to a host on the destination vehicle. The destination host replies an ICMPv6 echo reply. The period of time between the time the request is sent and the time the reply is obtained is measured at the sender side using *ping6*.

10.5.2 Throughput

The throughput is measured in UDP and TCP. It is measured with the *iperf* tool. In UDP, *iperf* is executed in both the sender and the receiver. UDP packets are set with a with fixed rate. The sender is not able to see the result because the communication is unidirectional from the sender to the receiver. The throughput is shown on the receiver side. On the other

[5] http://www.aerial.net/shop/product_info.php?cPath=35_37&products_id=510
[6] http://www.aerial.net/shop/product_info.php?cPath=35_37&products_id=172

hand, the sending rate is automatically adjusted with TCP's congestion control mechanism. The sending rate is adjusted depending on the acknowledgement messages received. The throughput appears in both the sender and receiver.

10.5.3 Jitter

The jitter is a measure of the variability over time of the packet latency across a network. A network with constant latency has no variation (or jitter). Packet jitter is expressed as an average of the deviation from the network mean latency. The value is displayed in *iperf* using UDP. Our AnaVANET evaluation tool (Section 10.8) computes it.

10.5.4 Packet Delivery Ratio (PDR)

The Packet Delivery Ratio (PDR) is the percentage of packets arrived at the receiver divided by packet sent by the sender *i.e.* the number of packets received by the destination divided by the number packets sent by the source. *iperf* shows it in the receiver side. AnaVANET described in Section 10.8 calculates the PDR on each one hop link between MRs as well as between hosts attached to source and destination MRs.

10.6 Indoor Evaluation Scenarios

In this section we describe the common scenarios for evaluating IPv6 over GeoNetworking. (See Chapter 12 and Chapter 13).

10.6.1 Direct Path Evaluation Network Configuration

We used the platform described in Section 10.2, however the tests were performed without vehicles. All the equipments shown in Figure 10.5 were settled on the desk in INRIA and the tests were performed without moving. In the indoor testbed, the MRs are put close to one another. In this case, the three MRs are in the same wireless range and each MR can receive the beacons from the others. As a result, at the IP layer, the destination receives redundant packets from both the forwarder (the relaying node) and the sender. To resolve this problem, the GeoNetworking layer configuration sets up some variables to filter the reception of the packets by their GeoNetworking ID. The scheme is implemented only for performing indoor evaluation. In actual case shown in Figure 10.5, *MR1* discards the beacons from *MR2* and vice versa. GPS positioning is disabled for indoor evaluations and static position is recorded in a configuration file instead. With the static configuration, MRs are located in a line. The distance between *MR1-MR3* and *MR3-MR2* was configured around 500 meters.

The scenarios of the tests are performed on MRs to evaluate the latency in the case of ICMPv6 traffic and the PDR and the throughput when transmitting UDP packets. *MNN1* runs a script to evaluate several performance metrics with changing various parameters. We evaluated single and multi-hop communications in the GeoNetworking domain. In the single hop tests, *MR1* and *MR2* are directly reachable. In the multi-hop test, the forwarding *MR3* is a GeoNetworking node that relays the message sent by IPv6 MNNs without involving the IPv6 stack.

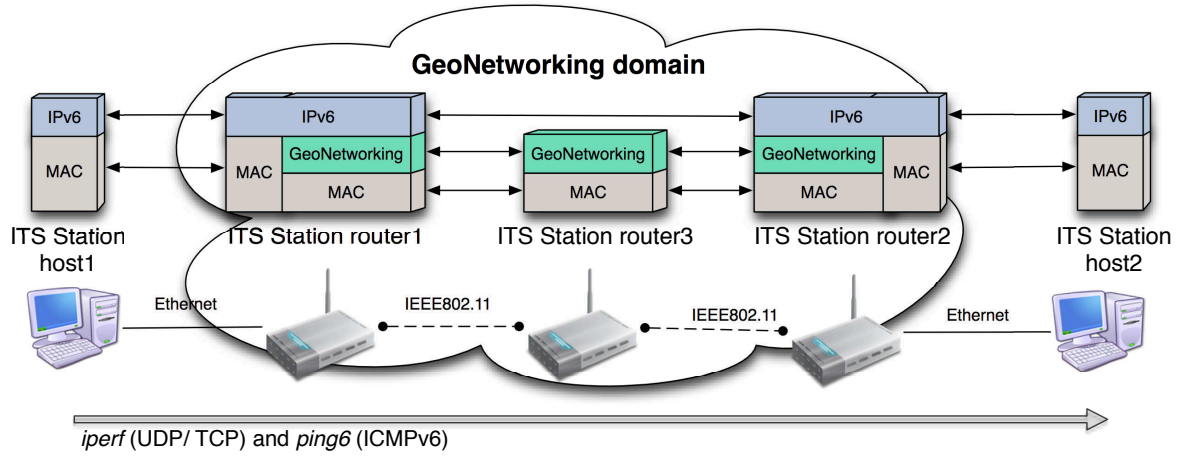


Figure 10.5: Indoor Network configuration

10.6.2 Anchored Path Evaluation Network Configuration

As well as direct path evaluation in the previous section, the anchored path evaluation is performed with the platform described in Section 10.2. The scenario is shown in Figure 10.6. The GPS data is not obtained from actual GPS device but is statically recorded in a configuration file. The traffic is generated by the *iperf* tool. The two communication end-points are one MNN attached to the MR that sends the traffic to be evaluated and a CN, considered to be located in the Internet. In these tests, packets transit via the HA. We evaluate two types of traffic: i) UDP traffic which is a unidirectional transmission flow from the source to the destination end-nodes where the considered metrics are the packet loss rate and the throughput, and ii) ICMPv6 traffic which is a bi-directional communication flow between the two end-nodes where the considered metrics are RTT and the packet loss rate.

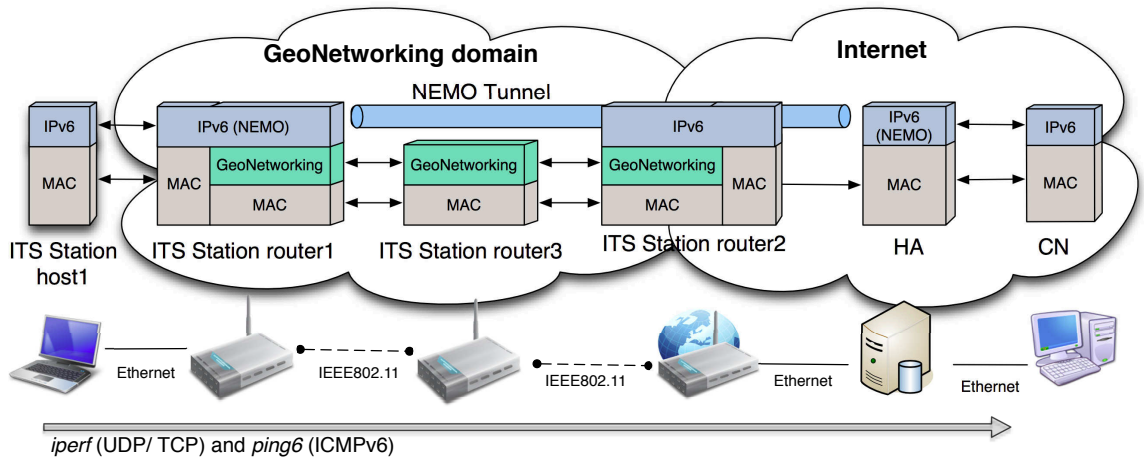


Figure 10.6: Network configuration of the indoor test

10.6.3 ICMPv6 latency evaluation

To evaluate the latency, we measured the RTT between the MNNs attached to the MRs. *MNN1* sends ICMPv6 Request every 0.1 second. The ICMPv6 packet is increased by 20 bytes. The packet size is varying from 20 bytes to 1500 bytes. Once the test is finished, the log file is parsed in order to get the maximum, the minimum and the average RTT as well as the packet loss for each packet size. In these tests, the log files are stored and parsed only on *MNN1*.

10.6.4 UDP packet delivery ratio evaluation

In this test, we evaluate the PDR in a UDP communication. We set up a UDP client attached to *MR1* that generates UDP packets and sends them to a UDP server attached to *MR2*. The UDP client and server save the log file traces. After the tests, the log files of both the client and the server are parsed through pointers as the used port number and the packet loss results are plotted. The UDP packets are generated at *MNN1* and sent to *MNN2* through wireless link between MRs. In this test the bandwidth is varying from 1 to 6 Mb/s. For each bandwidth value, the read-write buffer is increased from 20 bytes to 1900 bytes.

10.6.5 TCP throughput evaluation

In this test, the maximum throughput is measured using TCP traffic. We evaluate the throughput for three values of the TCP segment size: 400, 800 and 1200 bytes. For each value, the window size is increased from 200 to 1600 bytes. The TCP client is attached to *MR1* and the TCP server is connected to *MR2*. In this case, only the log file obtained on the server side is parsed and analyzed.

10.7 Outdoor Evaluation Scenarios

In this section we evaluate the network performance using the outdoor vehicular platform. The network configuration is almost the same as for the indoor experiments except that GPS is used to dynamically get vehicle position information and a network sniffer is used to retrieve packet information and paths. Real field evaluation is performed with the same equipment as for the indoor test, but also with a test fleet of four conventional vehicles (Citroën C3 shown on Figure 10.1).

A set of scenarios were considered taking into account several road parameters and constraints to render the scenario as realistic as possible. The main factors which determine these scenarios are:

- **Mobility**: Vehicle mobility is a key issue to cope with realistic VANET conditions. This way, we have considered static scenarios, to test the network operation in a controlled way, but also dynamic scenarios under common traffic situations. Of course, field operational tests should be conducted to confirm the experimental results taking into account proper handling of mobility, i.e. Doppler shifting, fast fading, etc.

- **Environment**: Urban and interurban environment affects communication performance, because the signal propagation is hidden by buildings (among other elements), and the line of sight between vehicles is not always possible. Two environments are considered in our tests: a semi-urban one located at INRIA-Rocquencourt, which contains a set of small buildings surrounded by streets, and a highway stretch, the A-12 autoway, near

INRIA-Rocquencourt. The tests are performed in the 2.4 GHz radio band due to lack of available hardware in the 5.9GHz radio band (IEEE802.11p). Also, the results are affected by the type of antenna. Field operational tests should thus be performed in the 5.9 GHz frequency band and with antenna diversity.

- **Number of vehicles**: The number of hops between the source and the destination vehicles affect the communication delay, as it was expected. In addition to the extra forwarding delay, the packet loss at MAC level also increases due to transmission interferences. Up to three vehicles are considered in the field trials, in order to check the increase of communication delay with the number of hops.

As summarized in Figure 10.7, Testing scenarios have been divided into urban and highway; mobility has been set to static, urban-like speed, and high speed; and a wide range of performance metrics have been used, such as bandwidth, RTT , jitter and PDR. The traffic types (UDP, TCP and ICMPv6) have been applied over each defined scenario.

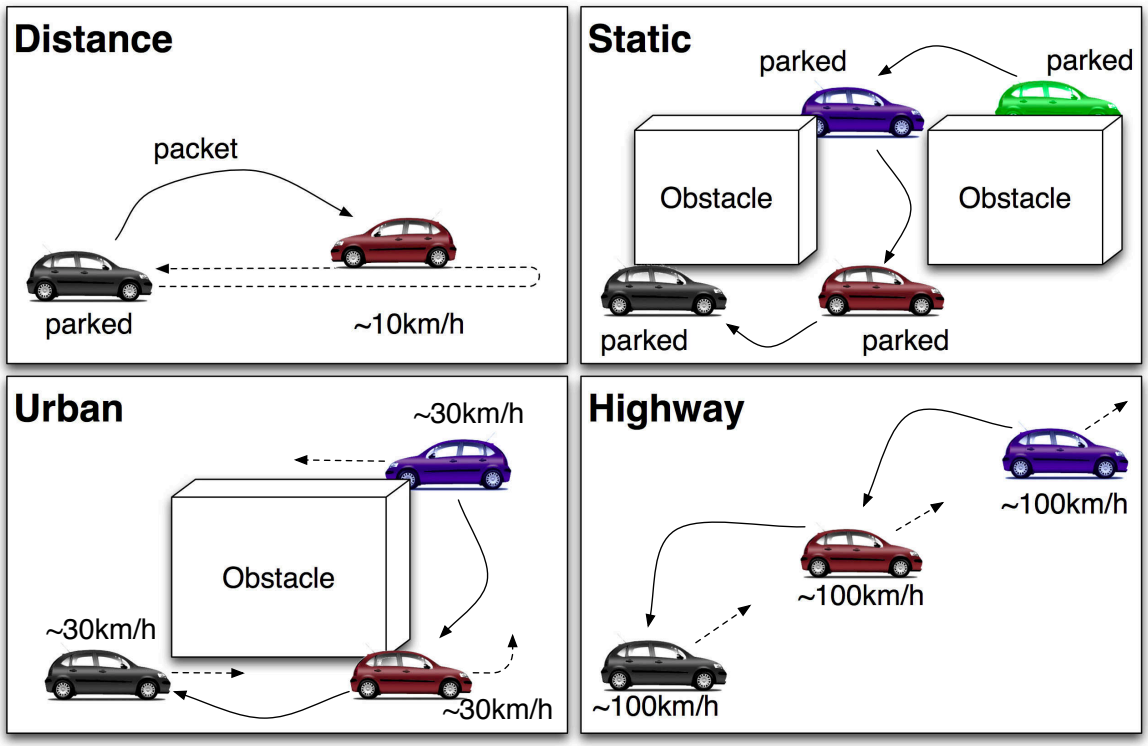


Figure 10.7: Real field Evaluation Scenarios

10.7.1 Distance Test

The distance test is performed with two vehicles as shown in Figure 10.7. In the beginning of the test, both vehicles locate at same points. Then, one vehicle does not move at the point and the other vehicle leaves straight from the point during the communication between them with slow speed (up to 10 Km/h). At some point the packet between them are dropped because of wireless radio range limitation, then the moving vehicle return to the first place. When the vehicle comes back, the packets are transferred again in the wireless radio range.

There is no obstacle between vehicles and the aim of this scenario was to check the maximum distance the wireless range can reach.

10.7.2 Static Test

As shown in Figure 10.7, Static test is performed with three or four vehicles. All of them are parked at the place during the test and they are connected with multi-hop manner because the buildings block the direct communication between source and destination vehicles. This test brings the network performance result of two hops and three hops away because the network topology of the vehicles are stable and there are no route changes during the test.

10.7.3 Urban Test

As shown in Figure 10.7, Urban test is performed with three or four vehicles that are moving slowly (up to 30 Km/h). The buildings or the other obstacles block wireless radio access between vehicles frequently. Because of the dynamic environment, the topology of the vehicle network is changed frequently. The aim of the test is to measure the network performance with the dynamic topology change and evaluate the effect of the obstacle that block the wireless radio between vehicles.

10.7.4 Highway Test

As shown in Figure 10.7, Highway test is performed with three vehicles. The vehicles run on a highway during the UDP, TCP or ICMPv6 communication is established between vehicles. The speed is up to 100 km/h. The distance is dynamically varying due to road traffic conditions. However building will not block the wireless radio frequently.

10.8 Evaluation tool: AnaVANET

AnaVANET is a tool developed at INRIA with Murcia University to analyze vehicular networks. It has originally been used to evaluate OLSR-based ad-hoc vehicular networks [Santa2009b, Santa2009a] . Then, AnaVANET has been extended in order to analyze IPv6 packets transmitted with a GeoNetworking header and NEMO header [GeoNet-D.7, Tsukada2010b].

We first present the system overview of AnaVANET in Section 10.8.1. Then, basic packet processing methods are described in Section 10.8.2.

The GeoNetworking extension is described in Section 10.8.3. Section 10.8.4 gives the details of AnaVANET NEMO extension to treat the packet with NEMO header and NEMO signaling (BU, BA and Binding Error (BE)). Initial AnaVANET was not designed for Internet-based communication, but only vehicle-based communication. This caused the problems especially in handover scenarios. The packet processing in the evaluation for handover scenarios is described in Section 10.8.5.

10.8.1 AnaVANET System Overview

Figure 10.8 provides an overview of the experimental evaluation process carried out in the tests. The Sender (MNN) is in charge of generating data traffic, and both the sender and the receiver record a high level log, according to the application used to generate network traffic. All MRs record information about forwarded data packets by means of the *tcpdump* software, and log the vehicle position continuously. All this data is post-processed by the AnaVANET

software and then analyzed. A Java application traces all the data packets transmitted from the sender node. This way, it is possible to detect packet losses and calculate statistics for each link and end-to-end, and merge all these per-hop information with transport level statistics of the traffic generator. As a result, AnaVANET outputs an Extensible Markup Language (XML) file with statistics over one-second periods, and a packet trace file with the path followed by each data packet.

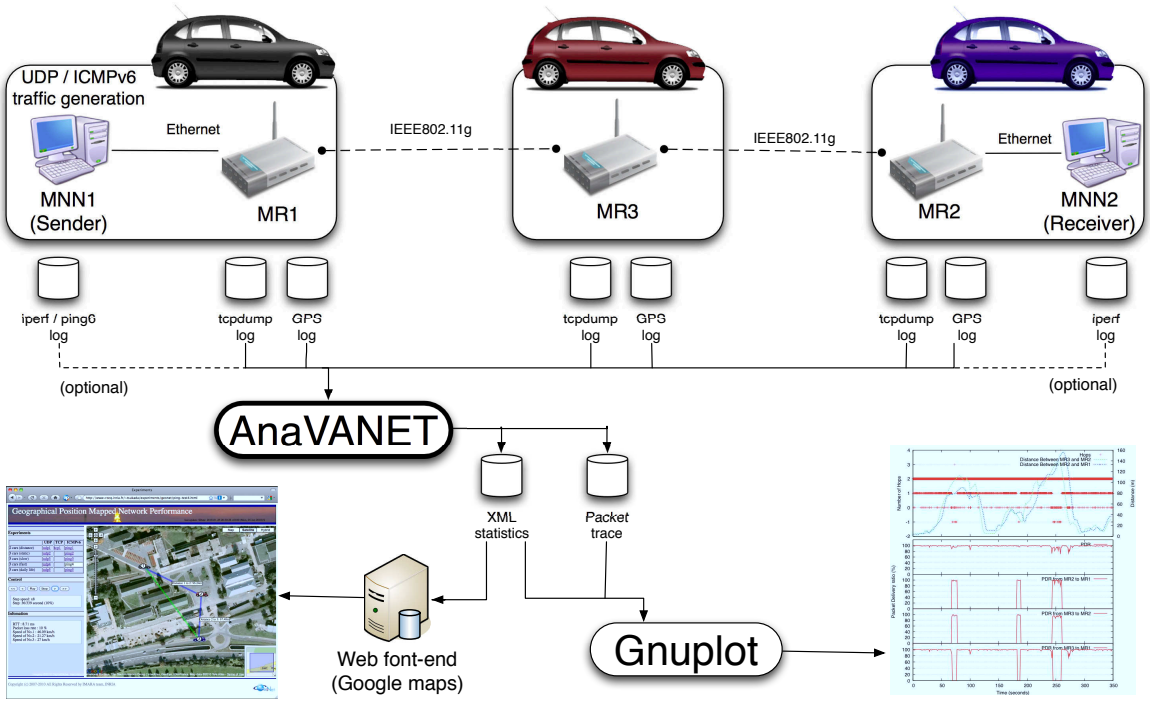


Figure 10.8: AnaVANET: Overview of packet processing and analysis

The experiments carried out are available on the websites and can be replayed on a map to see the momentary performance of the network during the tests. Figure 10.9–10.12 show screen shots of these websites. All the experiments can be selected and main performance metrics can be monitored at any time. Users can play and stop at any arbitrary point of the test with the control buttons on the left side of the page. The player speed, one step forward and one step backward are also implemented. On the map, the position and movement of the vehicle are depicted with the speed of each vehicle and the distance between them. The transferred data size, bandwidth, packet loss rate, RTT and jitter, for each link and end to end are displayed. The network performance is visualized by watching the width of links and the colors used to draw them.

AnaVANET has been used in network performance measurement for OLSR (Figure 10.9)[7] [Santa2009b, Santa2009a] and GeoNet project implementations (Figure 10.10)[8] [GeoNet-D.7, Tsukada2010b]. It is currently being used in CarGeo6 evaluation in INRIA (Figure 10.11)[9] [Toukabri2011] and Nara Institute of Science and Technology (NAIST) in Japan (Figure 10.12)[10] [Satoru2011].

[7] https://who.rocq.inria.fr/Manabu.Tsukada/experiments/vanet-jose/
[8] https://who.rocq.inria.fr/Manabu.Tsukada/experiments/geonet/
[9] https://who.rocq.inria.fr/Manabu.Tsukada/experiments/itsnet/
[10] http://dev.inet-lab.me/inet-doc/public/anavanet/

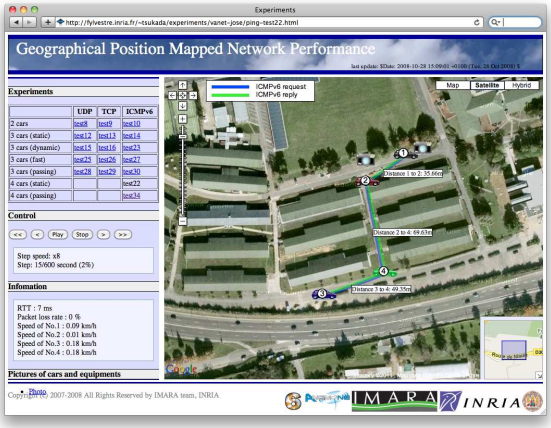


Figure 10.9: OLSR measurement

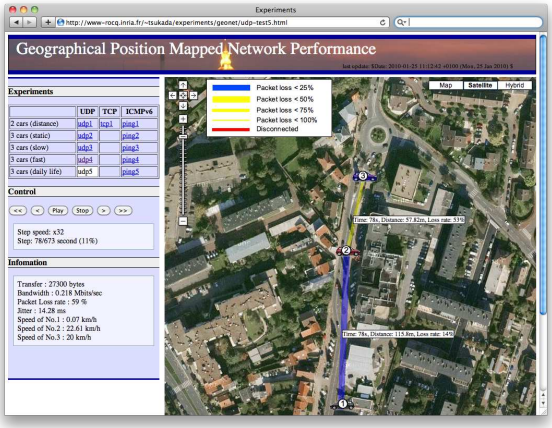


Figure 10.10: GeoNet measurement

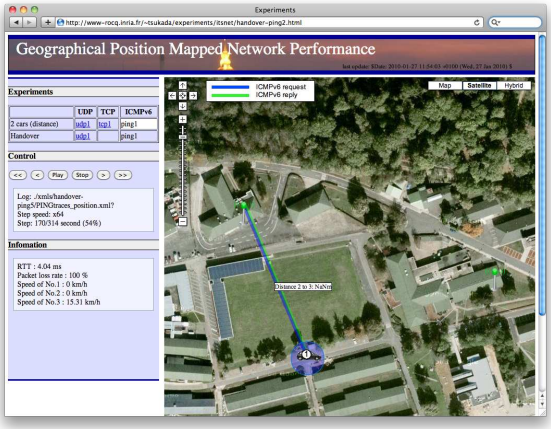


Figure 10.11: CarGeo6 measurement (INRIA)

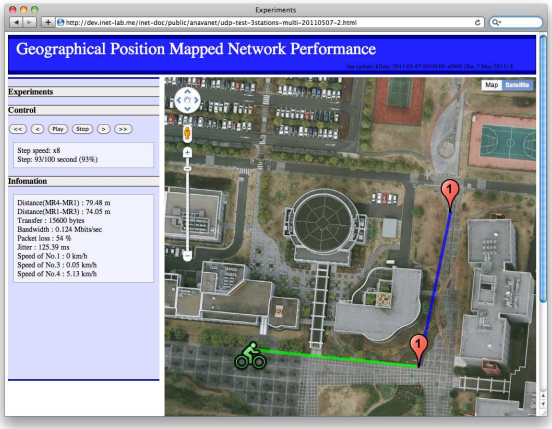


Figure 10.12: CarGeo6 measurement (NAIST)

10.8.2 Basic Packet Processing

After experiments, the *tcpdump* files and GPS files are collected from all the MRs to input the AnaVANET java software. The command in Figure 10.13 shows the case of ICMPv6 evaluation, however TCP and UDP evaluation shares the command except for the last line.

First line of the commend launches AnaVANET whereas other lines provide configuration parameters. The second line gives the information of the source MR where attached MNN generates the ICMPv6 echo request. The name of the MR, the MAC address of the egress interface, *tcpdump* log and GPS log (See Figure 10.15) are given as parameters. The line 3 and 4 are information of intermediate nodes, that line actually can be repeated for each intermediate node. The parameters of intermediate nodes are same as the seconds line. Line 5 configures the destination MR where the attached MNN receives the ICMPv6 echo request and reply ICMPv6 echo reply to the attached MNN to source MR. The parameters are described as well. The last line defines the test type (PING, UDP and TCP) and specifies the file of high-level log (the output of *ping6* or *iperf* software depending on the test type).

Figure 10.14 shows the functional modules of AnaVANET. Non-colored rectangles are the basic modules that the initial AnaVANET implementation had, and colored modules are

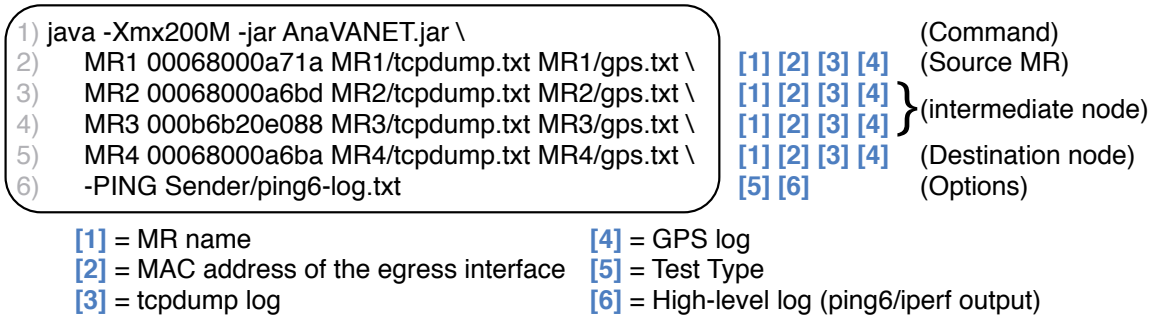


Figure 10.13: Command used to launch AnaVANET

extensions of GeoNetworking, NEMO and handover scenarios described in following sections. The packet processing starts from top, and the results of the processing is recorded to the per-packet trace file (text file) and per-second statistics file (XML file compatible with Google Maps). There are six steps in the AnaVANET processing as in Figure 10.14 such as GPS log processing, *tcpdump* log processing, packet tracing and statistics, high-level log matching and output file generation. AnaVANET traces the packets for UDP and ICMPv6, because TCP packets resent from MNN with same sequence number when the packet is lost. This makes mis-processing (double counting) for packet trace. TCP test only considers vehicles' position and end-to-end performance taken by *iperf* log (first, fifth and sixth step are considered in Figure 10.14.)

As a first step, AnaVANET processes GPS log. With the file, first, AnaVANET synchronizes the time between *tcpdump* log recorded with hardware time and GPS log that recorded with GPS time. The GPS log is described in National Marine Electronics Association (NMEA) format as shown in Figure 10.15. The hardware time recorded in *tcpdump* log has gaps between the MRs, because it is very difficult to synchronize the time of many devices for a long time in second order. On the other hand, the GPS time given by satellite is always synchronized when devices are located in almost same place. Thus GPS time is used for the rest of the calculation for the packet processing. The hardware time recorded in *tcpdump* file is calibrated with GPS time by calculating the gap between GPS and the hardware time in the beginning of the processing.

As shown in Figure 10.15, the line starts from $\$GPRMC$ in GPS file gives the position of the vehicle and speed. AnaVANET takes the data from GPS file and used for distance calculation between vehicles. The distances are calculated each second by *Haversine* formula (See Equation 6.1 for details).

At the next step, *tcpdump* log is processed. All the packets in the log are stored in the packet hash table with the time, source MAC address, destination MAC address, source IPv6 address, destination IPv6 address, packet type and sequence number. Only packets which match to the test type (ICMPv6, TCP, UDP) given in the command line option are considered while the other packets are ignored (*i.e.* beacons). The *tcpdump* log is a text file as shown in Figure 10.16 (It shows the case of ICMPv6 test). The first line shows important packet attributes including time, source IPv6 address, destination IPv6 address, packet type and sequence number. The time is recorded by the hardware time, thus it is converted to the GPS time and stored to the hash table. Then AnaVANET takes the source address and destination address from the first 48 bits and the next 48 bits.

At the next step (packet tracing), the packet is traced based on the MAC address stored

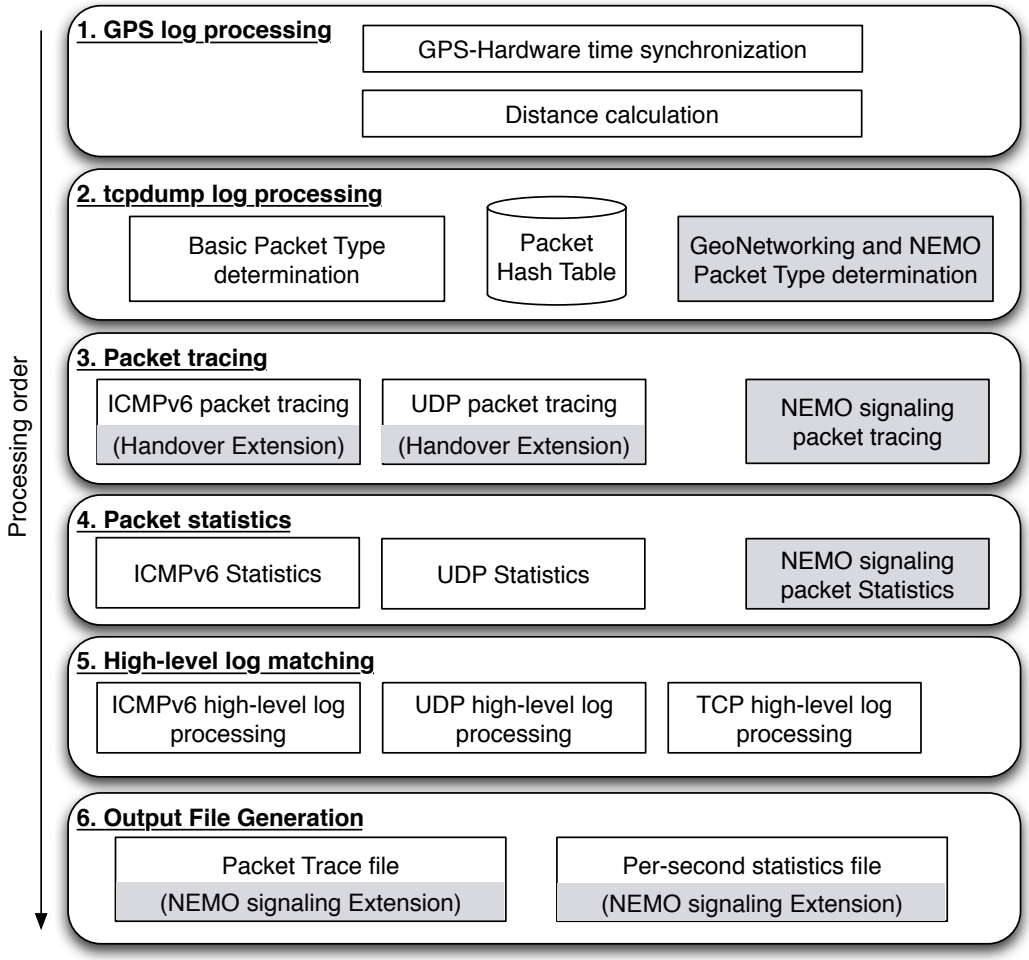


Figure 10.14: AnaVANET software modules

in the packet hash table. The trace starts from the sender MR and checks if the packet is received at the next MR correspondent to the destination MAC address of the traced packet. And the check continues successively until the packet arrives the destination given by the command. In the ICMPv6 case, the echo reply packet is matched with echo request by the sequence number. The check continues successively from destination MR until source MR receives the reply packet. The result is used for the per-packet packet log at step 6 (Output file generation) in Figure 10.14.

The Packet Delivery Ratio (PDR) of each link in each second are calculated. For example, in the scenario with three MR, all the links are MR1 → MR2, MR1 → MR3, MR2 → MR1, MR2 → MR3, MR3 → MR1 and MR3 → MR2. The PDR is calculated by the number of arrived packet divided by number of sent packets on the link.

At high-level log matching, AnaVANET processes the test file of output of ping6 or *iperf*. The result of the processing is matched to the previous result in packet statistics (step 4). In ICMPv6 test, the ping6 output in the sender is processed which includes the RTT between the sender and receiver in each second. In UDP, the *iperf* output in receiver side is processed that includes transferred bytes, bandwidth and jitter. In TCP test, the output of *iperf* is recorded in sender includes transferred bytes and bandwidth.

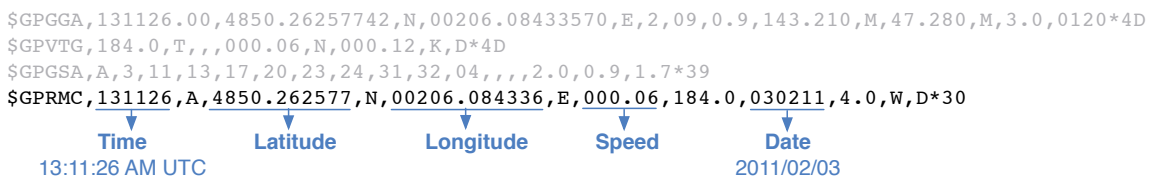


Figure 10.15: GPRMC sentence in GPS log

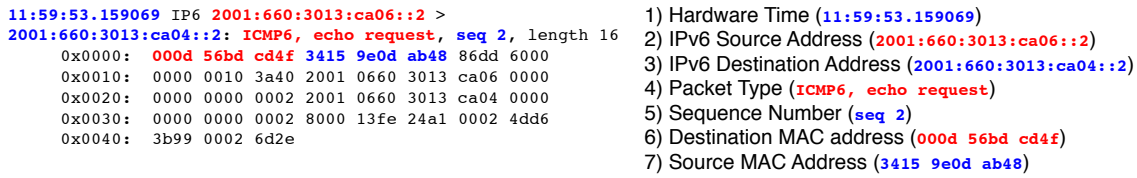


Figure 10.16: IPv6 native packet processing

Final step is two output files generation. One file for per-packet trace as a result of step 3, records the packet itinerary from source MR to the destination MR (it may drop somewhere) with the transmitted time and number of hops. This file is generated only for UDP and ICMPv6 test. The other file is for per-second statistics as a result of step 4 and 5. The file is XML format and can be used for displaying results on Google maps.

10.8.3 GeoNetworking Packet Processing

AnaVANET is extended to process the packet with GeoNetworking header. The extended module is packet type determination in *tcpdump* log processing (step 2) in Figure 10.14. In command line, $-GeoNet$ option switches using from Basic packet type determination to GeoNetworking packet type determination. The extended packet type determination considers 80 octets of the GeoNetworking header.

Figure 10.17 shows the example of GeoNetworking packet type determination. First of all, the first line of *tcpdump* log does not give the attribute of the packet unlike IPv6 native packet. The line gives only the recorded time and packet size. AnaVANET takes the source and destination MAC address from second line (line of $0x0000$).

In order to determine the packet type, it should see the next header field in the IPv6 header, which is marked $0x11 = 17$ in Figure 10.17. In the example, as the protocol number 17 means UDP, AnaVANET can determine the packet type (When the protocol number is $0x3a = 58$, it is ICMPv6 packet. The example is in the Figure 10.18 in next section). Then from the IPv6 header, the IPv6 source and destination address are taken. The first four digits of line $0x0090$ is sequence number of the UDP packet. The number is used as an identification number of the packet in AnaVANET. The packet information taken above is stored in the packet hash table as well as IPv6 native packet. The rest of the processing is common as described in Section 10.8.2.

10.8.4 NEMO packet Processing

NEMO extension to AnaVANET consists of two parts: packet type determination with NEMO header (actually IPv6 header, 40 octets) and NEMO signaling packet processing. The packet type determination with NEMO header is added to the *tcpdump* log processing (Step

```
11:13:07.960653 00:06:80:00:a7:0b > 00:06:80:00:a7:1a,
ethertype Unknown (0x0707), length 1442:
        0x0000:  0006 8000 a71a 0006 8000 a70b 0707 3002
        0x0010:  0002 9405 01ff 0000 0000 0000 ca06 67a8
        0x0020:  0000 f8a0 4917 f084 0001 0200 0000 f8cb
        0x0030:  0000 0000 0000 0000 ca06 67a8 0000 f8a0
        0x0040:  4917 f084 0001 0200 0000 f8cb 0000 0000
        0x0050:  0000 0000 ca04 0000 0000 0000 0000 6000
        0x0060:  0000 051c 113f 2001 0660 3013 ca06 0000
        0x0070:  0000 0000 0002 2001 0660 3013 ca04 0000
        0x0080:  0000 0000 0002 e898 1389 051c 831c 0000
        0x0090:  0003 4d3e a846 0000 5b3c 0000 0000 0000
        0x00a0:  0001 0000 1389 0000 0514 000f 4240 fffe
        0x00b0:  a070 3637 3839 3031 3233 3435 3637 3839
  ...(Skip)....
```

1) Hardware Time (11:13:07.960653)
2) Packet length (1442)
3) Destination MAC address (0006 8000 a71a)
4) Source MAC address (0006 8000 a70b)
5) Next Header (0x11 = 17 (UDP))
6) IPv6 Source Address (2001:660:3013:ca06::2)
7) IPv6 Destination Address (2001:660:3013:ca04::2)
8) Sequence Number (0x 0003 = 3)

Figure 10.17: Packet with GeoNetworking Header

2 in Figure 10.14). Regarding NEMO signaling processing, three parts are extended, that are NEMO signaling processing added to packet tracing (step 3), NEMO signaling statistics added to the packet statistics (step4) and NEMO signaling extension added to the output file generation (step 6). All the NEMO extension functions are activated with $-NEMO$ option in command line.

In *tcpdump* log processing (Step 2), the NEMO header should be considered for the packet type determination. Figure 10.18 shows the example of the packet with NEMO header and GeoNetworking header. The first line of the *tcpdump* log does not give the packet attributes except for the recorded time as well as in the previous section, because it is also encapsulated with GeoNetworking header. The source and destination MAC address are given in the first line as well. After GeoNetworking header the IPv6 header appears (the line of $0x0060$). The next header field ($0x29 = 41$) in the line shows that the packet is encapsulated by IPv6 header (NEMO header). When AnaVANET discovers the NEMO header, it looks inner packet in order to determine the packet type. After 40 octets of NEMO header, it shows the inner IPv6 header. In the example of Figure 10.18, the next header field of inner IPv6 header has $0x3a = 58$ that means that next header is ICMPv6. The first 2 digits of the next header shows that the packet is whether ICMPv6 echo request ($0x80 = 128$) or ICMPv6 echo reply ($0x81 = 129$).PAt that point, the packet type is determined completely, and then the sequence number is taken from line of $0x00b0$ used as the identifier of the packet in the rest of the processing.

The NEMO signaling packet (BU and BA) is also processed when the $-NEMO$ option is enabled. The example of BU is illustrated in Figure 10.18. As well as the other packet with GeoNetworking packet, the recorded time, source MAC address and destination MAC address are detected. Then it checks the next header field in the IPv6 header. In the case of BU, destination option ($0x3c = 60$) is specified in the field. (In the case of BA, IPv6 routing header ($0x2b = 43$) is specified). In both cases of BU and BA, the payload protocol is specified as mobility header ($0x78 = 135$). The sequence number of the BU and BA is used as identification number to match the correspondent NEMO signaling message. The packet information is stored in the packet hash table as well as the other packets.

The other function of NEMO extension is tracing NEMO signaling and statistics. The NEMO signaling is traced in order to analyze if the binding registration is terminated successfully or not, and where the signaling packet is dropped at packet tracing (step 3). First, the BU sent from source MR is traced successively by source and destination MAC address until arriving at the destination node (Access Point (AP)). When the BU arrives at an AR, the correspondent BA is also traced until it reaches to the source MR. The two-way packets

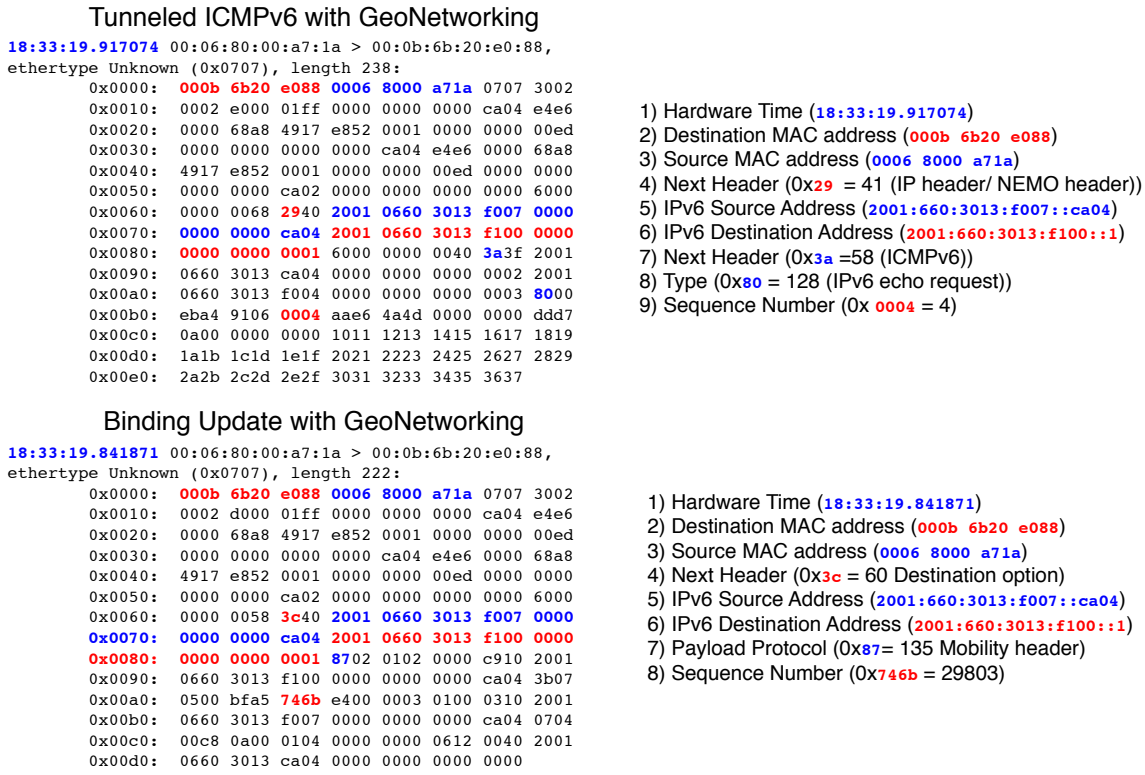


Figure 10.18: Packet with NEMO and GeoNetworking

trace file (BU and BA) is generated in the step 6 in Figure 10.14.

As NEMO signaling status, whether of three statuses is recorded in the per-second statistics that are, NEMO signaling not sent (0), NEMO signaling successful (1) and NEMO signaling unsuccessful (2).

10.8.5 Processing for Handover Scenarios

AnaVANET was initially designed for analyzing unicast vehicle-based communication. Thus the source MR and destination MR are given in the command line. This does not cause problem in the case of roadside-based communication, however there are problem in the Internet-based communication because there is multiple exits (destinations) from VANET point of view in the case of handover between APs. The packet from source MR goes out of VANET at an AP, but the AP may change depending on the movement of the vehicle. Thus the AnaVANET trace system should have multiple destinations. The multiple designation are specified as $-destMR\,number$ option in the command line. With this option, it traces the packet until reaching the specified destination in packet trace (Step 3). The ICMPv6 packets (echo request and reply) and NEMO signaling (BU and BA) are traced from the selected destination to the source MR.

Chapter 11

Evaluation of Simultaneous usage of Anchored and Direct Paths

Contents

MANEMO, *i.e.* the combination of MANET and NEMO offers a number of benefits, such as route optimization or multihoming. With the aim of assessing the benefits of this synergy, this chapter presents a policy-based solution to distribute traffic among multiple paths to improve the overall performance of a vehicular network. An integral vehicular communication testbed is developed to carry out field trials. First, the performance of the Optimized Link State Routing (OLSR) is evaluated in a vehicular ad-hoc network with up to four vehicles as a benchmark in order to compare with IPv6 GeoNetworking under the same conditions in the next chapter. AnaVANET is used to analyze the impact of the vehicles' position and movement on the network performances. Performance results have been geo-located using GPS information. Second, by switching from anchored path (NEMO path) and direct path (OLSR path), paths between vehicles are optimized and the final performance is improved in terms of latency and bandwidth. Our experimental results show that the network operation is further improved with simultaneous usage of NEMO and MANET.

11.1 Performance Evaluation of OLSR

11.1.1 Experimental Setup Details

Performance Evaluation of OLSR is performed with up to four vehicles using LaRA testbed version 1 as described in Section 10.3.2. All of these test results were conducted by the AnaVANET tool shown in Section 10.8.

The results of this experiment (along with the rest of performed trials) is available on a public website [1], and can be replayed to graphically show the performance of the network during the tests.

The timing parameters of the OLSR daemon installed in MRs have been modified as shown in Table 11.1, to accommodate mobility conditions of a vehicular network. These modifications enable MRs to discover topology changes more quickly.

Parameter	Value	(default)
HELLO interval	0.5 sec	(2.0 sec)
HELLO validity	6.0 sec	(6.0 sec)
HNA interval	3.0sec	(5.0sec)
HNA validity	9.0sec	(15.0sec)

Table 11.1: Parameters for OLSR

11.1.2 Distance Test

Distance tests have been performed with two cars. The sender starts leaving from the receiver vehicle position (static), and then it comes back, at about 180 meters, to approach again to the initial point. The speed of the sender was maintained less than 10 Km/h to smoothly check the loss of connectivity.

Figure 11.1 shows PDR in the case of the UDP transmission. Packets start to be dropped around 100 meters of distance. The last packet arrives around 120 meters away and, after this point, there are no delivered packets, until the sender vehicle comes back and reaches 100 meters of distance. Since periodical OLSR control messages are lost when the distance

[1] https://who.rocq.inria.fr/Manabu.Tsukada/experiments/vanet-jose/

is around 120 meters, the path is removed of the routing table and the transmission ends at this point. The jitter in the same test is illustrated in Figure 11.2. When the sender car leaves the receiver one, at a distance between 75 and 120 meters, the jitter is higher, due to layer two retransmissions caused by the increase of the distance. When the sender approaches the receiver again, this effect is again visible at distances between 100 and 50 meters. It is noticeable how the communication is lost at a point further away than when the communication comes back. This is due to timeout periods in the reception of control messages give an extra time to maintain the communication link. When the vehicle comes back, some signaling traffic must be also exchanged before the routing table of the sender vehicle is updated.

The TCP performance over the same scenario is shown in Figure 11.3. As can be seen, only a one-way path has been logged. When the route is lost at 100 meters of distance, the TCP timeout expires and the transport layer link is broken. Finally, Figure 11.3 shows the RTT values collected in a Ping test over the same scenario, measured end to end. The base line of RTT is about 10 ms, but several peaks appear even under good conditions, due to route updates carried out by OLSR and the movement of the sender vehicle. The communication is again lost at a similar distance to the previous cases, however, it comes back earlier than in the UDP test. This is due to the network overhead is much lower in the Ping test (only one message per second), hence the OLSR signaling messages can be efficiently sent and the communication is reestablished earlier.

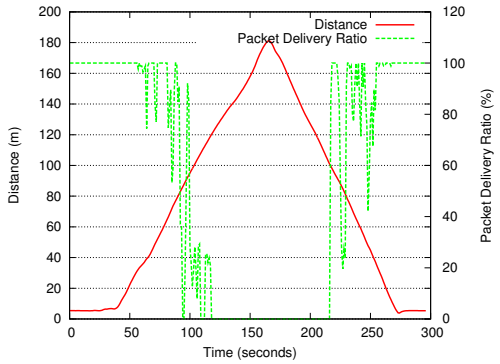


Figure 11.1: UDP range test with 2 cars (distance/PDR)

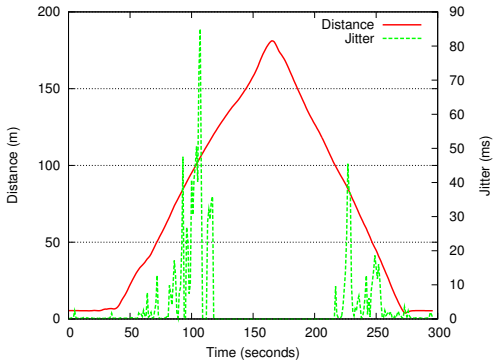


Figure 11.2: UDP range test with 2 cars (distance/jitter)

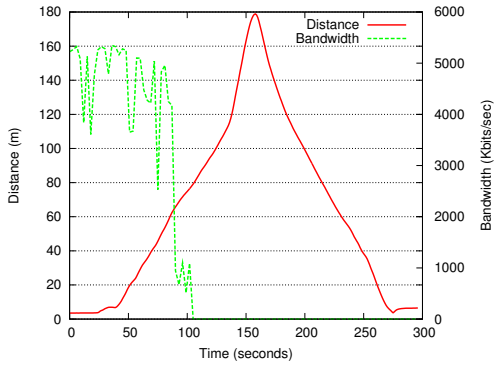


Figure 11.3: TCP range test with 2 cars (distance/bandwidth)

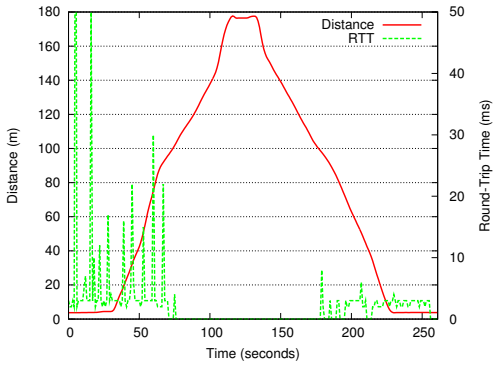


Figure 11.4: Ping range test with 2 cars (distance/RTT)

11.1.3 Static Test

Static test results are summarized in Table 11.2, using three and four vehicles, respectively. The total distance between the sender and receiver cars was 120 meters (70 plus 50 meters) in with three vehicles, and 155 meters (50 plus 70 plus 35 meters) with four vehicles. As can be seen, the UDP performance is almost ideal. Packet losses are not frequent, and the mean PDR is 99.99%. Small variances of performance are only due to route updates, noticeable in jitter values. In TCP results, the average bandwidth is 1.9 Mbps, what reveals a good performance too. However, frequent variations are evident if the standard deviation (STD) is considered. This is due to the operation of the TCP protocol, because the vehicles are static and the network topology does not present variations. According to slow start mechanism, TCP dynamically adjusts the transmission rate, but this algorithm does not converge, due to special features of wireless communications (mainly packet losses) and the presence of eventual route updates.

Ping tests show the good two-way latency of the network. With three vehicles, the average RTT is 4.96 ms, but this value is exceeded when four vehicles are considered, reaching a mean RTT of 7.25. Hence, the addition of one hop increments the latency by more than 2 ms. The RTT standard deviation is also higher in the last case, due to the new node imply additional control traffic and, overall, new occasional route updates. Moreover, since the route from the source to the destination terminals comprises a linear path across the four MRs, as the number of nodes increases, the probability of finding routing or delay problems along the path is higher.

Test	Metric	Min.	Ave.	Max.	STD
UDP 3 v.	PDR (%)	98.84	99.99	100	0.11
	Bandwidth (Kbps)	545.20	1001.59	1020.8	34.15
	Jitter (ms)	0.14	0.57	5.57	0.78
TCP 3 v.	Bandwidth (Kbps)	327.68	1915.95	2282.24	359.1
ICMPv6 3 v.	RTT (ms)	4.00	4.96	23	1.38
ICMPv6 4 v.	RTT (ms)	6.00	7.25	19	1.49

Table 11.2: Network performance in static tests

11.1.4 Urban test

This area contains a set of small buildings surrounded by streets, as can be seen in Figure 11.5 (The urban test described in Section 10.7.3). The four streets shown in the image, which round three of the buildings, have been chosen for this scenario. They stand in a 100 × 100 m square area. Three vehicles have been driven around the buildings, trying to block the direct link between cars one and three. The speed of the vehicles was kept between 15 and 30 km/h. The right and left roads visible in Figure 11.5 are very narrow and some communication problems were experienced when approaching the corners.

The results collected in the UDP tests are plotted in Figure 11.6. The several graphs show the results collected during four tests around the buildings. The upper plot shows the number of hops used in the paths followed by UDP packets, whereas the lower graphs show the end-to-end and per-link PDR. PDR is computed every second, while the number of hops is plotted for each packet transmitted from the sender node. When no hops are drawn, the route to the destination vehicle is not available. Zero hops means that the packet was sent

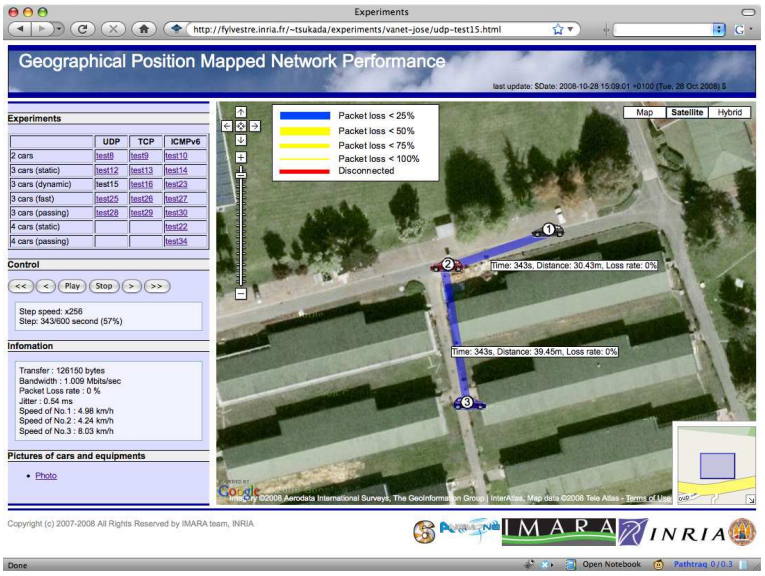


Figure 11.5: AnaVANET screenshot. Buildings avoid a direct line-of-sight communication, thus forcing the usage of multi-hop routes.

by the first MR, but was not received by any other. Negative values represent those packets that did not arrive to their destination, but reached some intermediate hops.

As can be seen, a direct relation exists between PDR and number of hops. When the number of hops is equal to or lower than zero, PDR decreases. When the vehicles drive along the same street, some direct paths (one hop) appear. On the contrary, when the distance between the sender and the receiver cars is large enough, the two-hop routes are used. These different types of paths can also be observed with the per-link PDR. Whereas the direct link (*MR3-MR1*) gives intermediate PDR values, the PDR between consecutive vehicles is almost identical and close to 100% when the two- hop link is used, due to the lower distances between nodes.

The performance obtained in the scenario has been analyzed according to the location of vehicles: corner and straight road. As can be seen in Figure 11.7, each corner is called SE, NE, NW, SW, according to its position (i.e. South-East for SE). In the same way, straight roads have been assigned the names E, N, W, S. Numbers below corner and road names indicate the time in which car 2 (vehicle in the middle) passes these points. For example, for SE, numbers 97, 257, 419 and 537 mean that car 2 passes the SE corner at times 97 s, 257 s, 419 s and 537 s. At these times the sender vehicle is at the next road (E in this case) and the receiver vehicle is at the previous one (S). On the other hand, when the middle vehicle is at a straight road, the sender vehicle reaches the next corner and the receiver vehicle is at the previous corner. The driving order is SE - E- NE - N - NW - W - SW - S, and three and a half complete rounds have been considered. The analysis starts at time 97 s at SE corner, and it ends at 594 s at NW.

As can be seen in Figure 11.7 the throughput obtained has been mapped with corner and straight road segments, and it has been analyzed for each round at periods of $\pm$ 10 seconds. A dotted line shows the result of each trial considered in the segment, and a bold line shows the average bandwidth. One can notice the two different bandwidth patterns obtained at corners and straight roads. Communication performance increases in corner scenarios, while it decreases at straight roads. When the intermediate vehicle reaches a corner, the direct

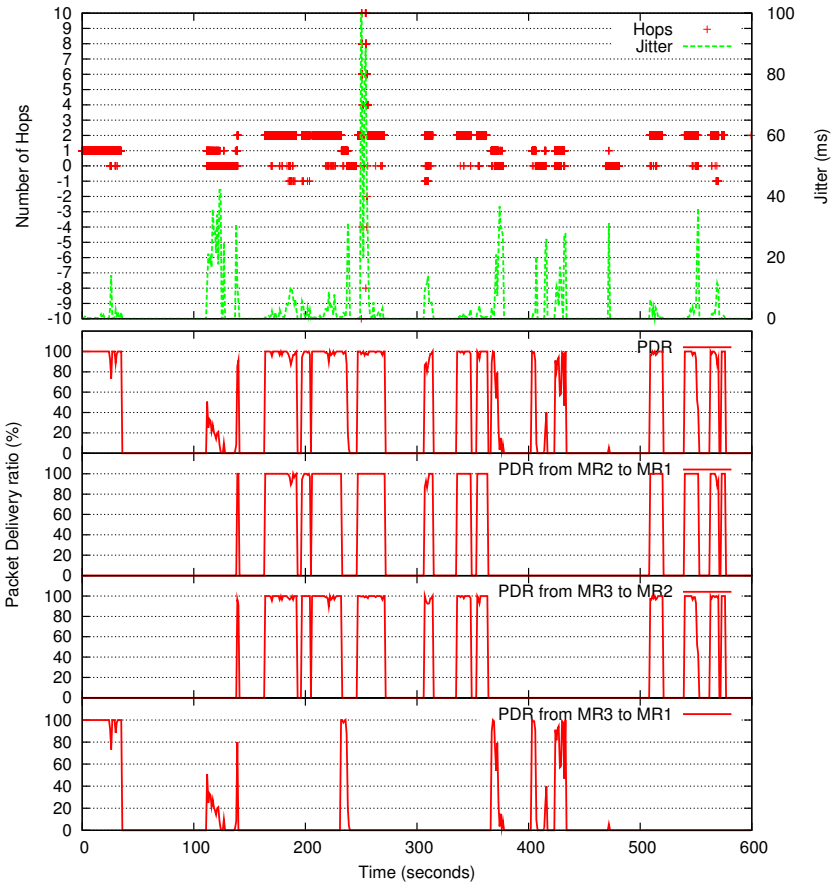


Figure 11.6: UDP urban test with 3 dynamic cars

path between the source and the destination vehicle is blocked, thus a multi-hop route is established in the network. At this moment, a good bandwidth is noticeable. When the heading vehicle turns again in the next corner, a multi-hop route still maintains connectivity but, as soon as car 3 and 2 cannot maintain the communication link, the network performance falls. This can be seen in the last ten seconds of straight road graphs in Figure 11.7. The effect of loosing the link between vehicles 2 and 1 is also present when the intermediate vehicle left the corner (last seconds of corner graphs and first seconds of straight road graphs), but it is less noticeable, since these two vehicles were arbitrarily driven more closely during tests.

Results obtained for segment W shows a different behavior than for the rest of straight roads. This is explained by the special physical conditions of the environment. First, this stretch comprises a narrow street surrounded by buildings on both sides. As can be seen in Figure 11.5, these conditions are only present in this segment, since the rest of roads have a clear space on one side. This fact enables the reflection of signals on the various walls. Moreover, the second interesting condition identified in road W is the greater altitude of the sender car with regard to the receiver car, when these are located near corners NW and SW, respectively. About five meters of altitude difference increases the packet reception probability, and a direct path between cars 1 and 3 is even noticeable at this segment. This can be checked at time 367 s in Figure 11.6. It is interesting to note that buildings on this INRIA area are quite low, about 3.5 meters, what complements the altitude effect. The rest of direct paths collected in the trials belong to segments S and E, which do have open areas

on one of the sides.

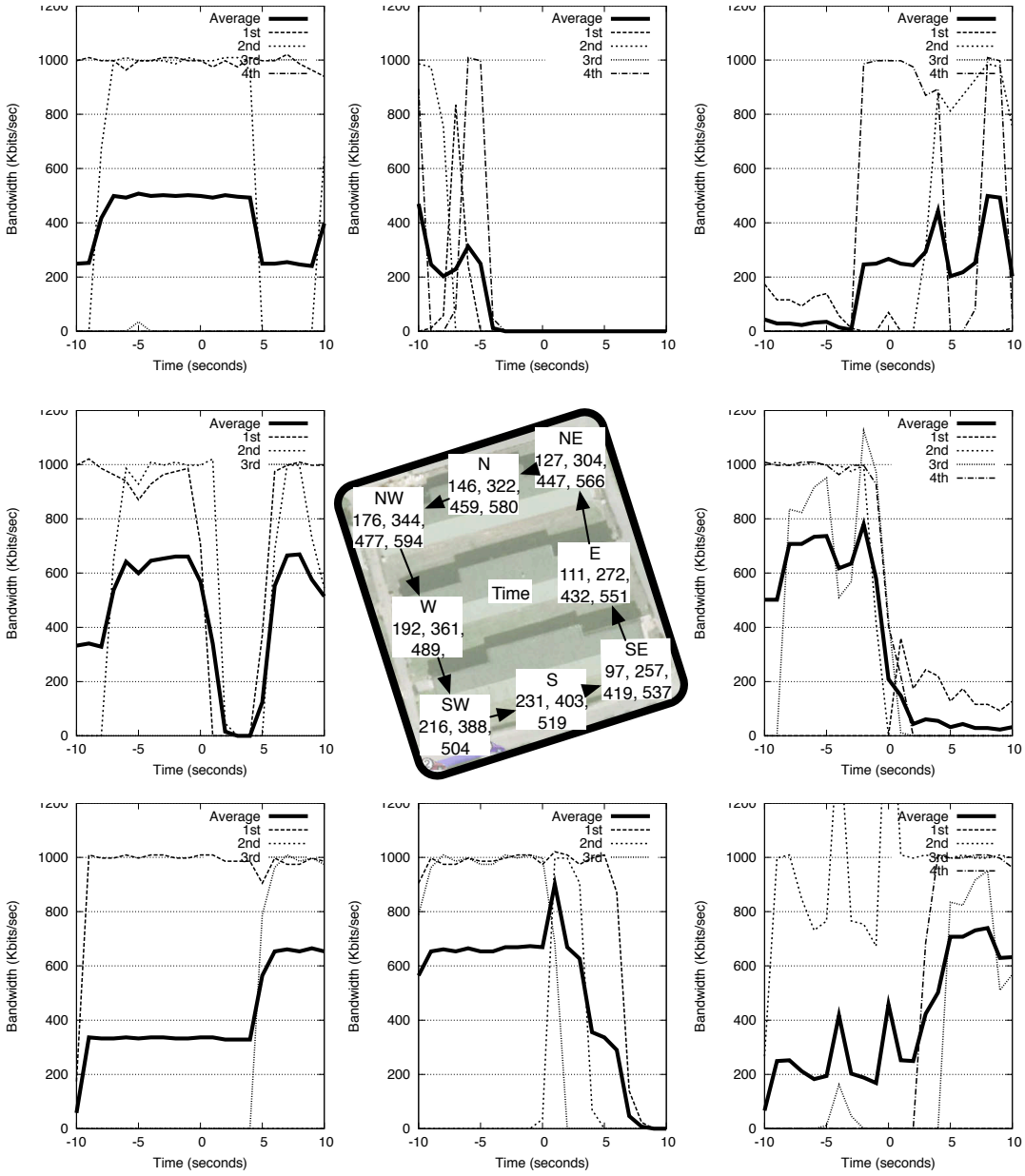


Figure 11.7: Network throughput at corners and straight roads for the UDP multi-hop test

The bandwidth obtained in the TCP test is shown in Figure 11.8. The performance of the network is very good in the first fifty seconds, due to the vehicles started the trial parked very near. However, the rest of the test shows a high variability, due to continuous changes in topology and communication problems in corners. When conditions are favorable, TCP try to normalize the bandwidth, but soon a link disappears and the bandwidth falls. Peaks of performance are obtained when the sender and receiver cars are in a direct line of sight. TCP timeouts do not expire because there are no long disconnection periods; hence the transport-level communication is maintained.

The final test (Figure 11.9) comprises a Ping transmission. As can be seen, several steps appear between two main RTT values: five and seven milliseconds. This matches with two-hop and four-hop two-way paths. Several three-hop routes have been collected, due to, the ICMPv6 Echo Request packets take a different path than the Echo Reply ones. If the ratio of non-delivered packets (negative hop counts in this case) is compared with the one obtained in the UDP test, it is noticeable how it is lower now. Since the data traffic is much more lower in the Ping case (one message per second), signaling traffic is more efficiently propagated, and changes in network topology are earlier known.

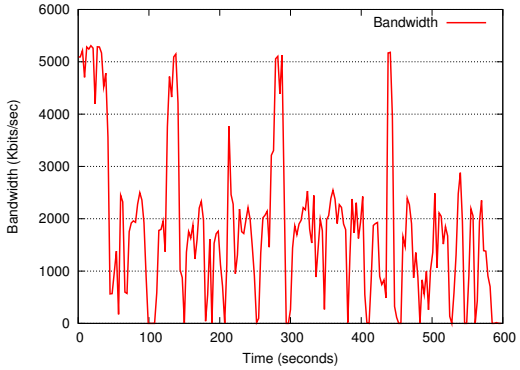


Figure 11.8: TCP urban test with 3 dynamic cars (bandwidth)

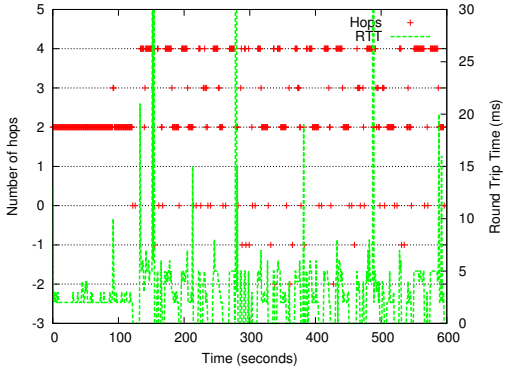


Figure 11.9: Ping urban test with 3 dynamic cars (hops/RTT)

11.1.5 Highway test

The highway test is performed with three vehicles as described in Section 10.7.4. The speed of the cars was around 100 km/h, but the distance between vehicles was variable, due to the rest of traffic on the road. Moreover, communication problems in this test are not only due to buildings, but also to surrounding vehicles.

The PDR obtained in the UDP test is presented in the lower part of Figure 11.10. As can be seen, when the distance between vehicles increases, the PDR becomes lower. As in the urban scenario, intermediate values between 0 and 100% are not very frequent; since OLSR removes the routes between nodes when signaling packets are lost. At the beginning, the network performance is good, because the direct path is chosen, as can be seen in the partial PDR study of the *MR3-MR1* link. When vehicles start to separate, the two-hop path is used, as it is shown in the PDR of *MR2-MR1* and *MR3-MR2* links and the number of hops of chosen paths, shown in the upper graph. High variations of distance provoke route updates and, therefore, packet losses. Around 300 seconds of test, vehicles regroup, but the three-hop path is maintained, because OLSR needs to adapt to the new topology. The high variability of distance around time 350 seconds, makes the network does not stabilize and many packets are lost. A higher period of 0% of PDR is noticeable, however, around 150 seconds of test. In this case, the communication between the sender vehicle and the others is blocked by a near building.

The bandwidth results of the TCP test are shown in Figure 11.11. Now the vehicles are grouped at the beginning of the tests and the bandwidth is around 5 Mbps. However, when Car 3 enters the highway and the distance with the other two cars increase, the bandwidth dramatically falls. As can be seen during the whole test, there is again a direct relation

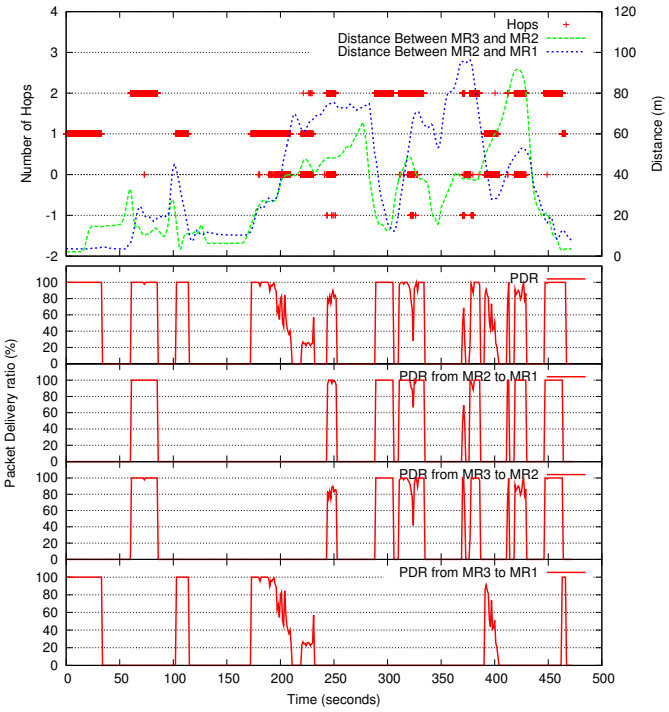


Figure 11.10: UDP highway test with 3 cars

between the distance of vehicles and the final performance. Taking into account the maximum range and static tests, it is easy to identify in the graph the moments in which a three-hop path is used. Bandwidths around 2 Mbps represent these cases, whereas results between 4 and 5 Mbps belong to direct paths.

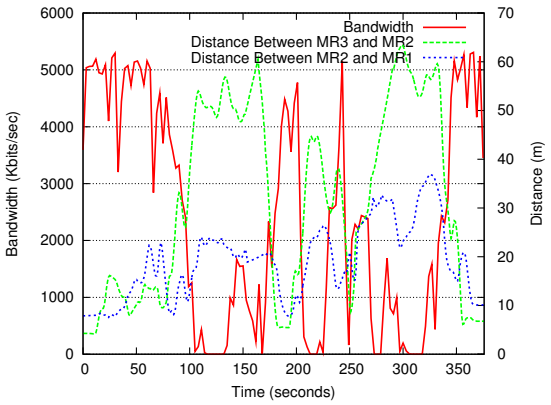


Figure 11.11: TCP highway test with 3 dynamic cars (bandwidth/distance)

Finally, Figure 11.12and 11.13 show the results collected during the Ping test. As can be seen, the RTT increases when the vehicles are far enough to use a four-hop two-way route. At this moment, the RTT passes from around three milliseconds to reach the five milliseconds. It is advisable again, how intermediate RTT values are not frequent, being the number of hops the main factor which determines the result. When the distance among vehicles grows and communication starts to be difficult, the links between MRs break, due to losses of OLSR

signaling messages.

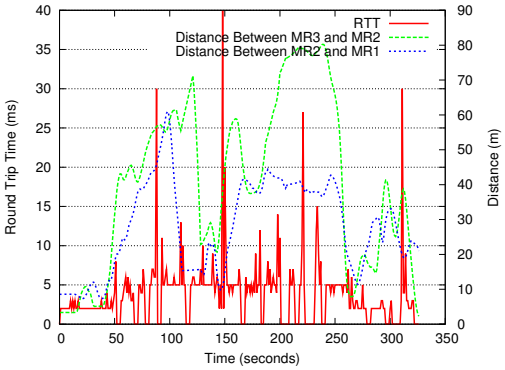


Figure 11.12: Ping urban test with 3 dynamic cars (hops/RTT)

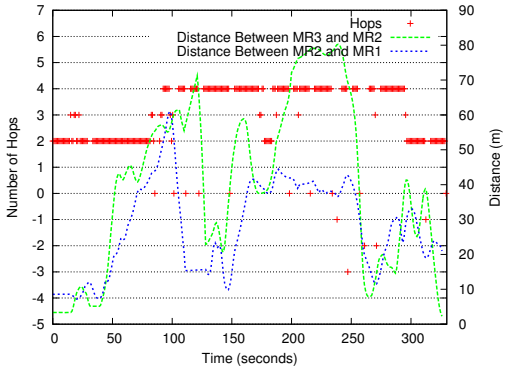


Figure 11.13: Ping urban test with 3 dynamic cars (hops/RTT)

11.2 Performance Evaluation of Simultaneous usage of NEMO and OLSR

For the case of the MANEMO subsystem described in Section 9.2, measurements of latency and throughput have been collected using both the VANET and the infrastructure segments of the testbed described in Section 10.3.1. This tests were performed using LaRA testbed version 1 as described in Section 10.3.2. A set of indoor and outdoor experiments have been conducted also at the Rocquencourt campus of INRIA and this section presents and analyzes most interesting results.

11.2.1 Experimental Setup Details and Initial Tests

As was done for VANET-only experiments, OLSR settings have been adjusted with the values shown in Table 11.3. These have been chosen to maintain a trade-off between the delay experimented when a topology change occurs and the network overload that implies control messages. Signaling traffic, apart from reducing the effective bandwidth of the network, it consumes computation resources on the nodes. For these experiments, OLSR settings have been adjusted to be aware of topology changes faster than in VANET-only tests in Section 11.1, with the aim of performing fast route changes between NEMO and OLSR.

Parameter	Value	(default)
HELLO interval	0.5 sec	(2.0 sec)
HELLO validity	1.5 sec	(6.0 sec)
HNA interval	1.0sec	(5.0sec)
HNA validity	3.0sec	(15.0sec)

Table 11.3: Parameters for OLSR

Some initial tests were performed to check the operation of the network. One issue that had to be solved was radio interferences between 802.11b managed and ad-hoc networks. Even when channels were chosen with a good distribution the problem persisted. To overcome this

drawback, the bandwidth of *MR1* interfaces were limited to 2 Mbps using a Linux' Quality of Service (QoS) system based on *tc* (Traffic Control)[2]. Network performance measurements under static conditions, and without any policy, between *MNN1* and *MNN2* are summarized in Table 11.4, including three different routes. RTT results is the average of 100 packets of ICMPv6 between MNNs and throughput results have been obtained averaging results obtained during a total of ten minutes of TCP tests. As can be seen, the results of the 3G link offer the worse results, due to the delay of the operator's network and the bandwidth limited by the radio coverage and the available resources in the cell. The 802.11b link improves these results, offering bandwidth capabilities equivalent to the ad-hoc case. However, the delay induced by the managed mode and the relay access point impact on the RTT results.

Path & interface	RTT	Throughput
NEMO over 3G	279.43 ms	416 kbps
NEMO over 802.11b managed	32.74 ms	1977 kbps
OLSR over 802.11b ad-hoc	8.58 ms	1987 kbps

Table 11.4: Performance of the MANEMO system under static conditions and depending on the Path type

11.2.2 Indoor Test

The policy-based MANEMO system has been firstly evaluated in an indoor testbed, to avoid interferences of other equipments and difficulties to trace the movement of MRs. The following experiments have been performed without any vehicle. Neither MRs nor MNNs have moved during a reference experiment of 300 seconds. It clearly demonstrates the performance expected for longer times or subsequent trials.

MNN1 has three addresses (A, B and C) in the MNP, and *MR1* distributes traffic from the mobile network via multiple paths depending on the source address. Packets from source address A or to port number 5102 are always forwarded via the 3G interface. Those from source address B or to destination port 5101 are routed via the Wi-Fi managed interface when it is available. Otherwise, they are forwarded over the interface. Traffic from source address C or to destination port number 5009 is transmitted via whatever available interface, prioritizing the most efficient (i.e. prefer ad-hoc to managed Wi-Fi and only use 3G if no other link is available). Table 11.5 summarizes these policies and indicates priorities in case several paths can be chosen. *MR2* distributes returning flows into its managed and ad-hoc interfaces according to the third policy, since it does not have any 3G interface. The HAs distribute flows to match these policies and avoid asymmetric paths.

For this indoor experiment, connection and disconnection events have been created using a shell script and common system tools. From $t = 0$ to $t = 60$, both Wi-Fi managed and ad-hoc interfaces of *MR1* are down. At $t = 60$, the managed interface comes up. At $t = 120$, the ad-hoc one is made available. From $t = 120$ to $t = 180$, all the interfaces are up and running. At $t = 180$, the ad-hoc link is turned off. At $t = 240$, the managed one is also switched off. The 3G interface is always available throughout the test.

[2] http://www.linux-foundation.org/en/Net:Iputils

Policy	Targets	3G	Managed Wi-Fi	Ad-hoc Wi-Fi
Always 3G	Source address A or destination port 5102	1	×	×
3G or managed	Source address B or destination port 5101	2	1	×
Any interface	Source address C or destination port 5009	3	2	1

Table 11.5: Flow distribution policies for MR1 (Smaller numbers reflect higher priorities)

11.2.2.1 Latency Measurements

To measure the RTT between MNNs, *MNN1* sends 56 Bytes ICMPv6 echo request packets from all addresses (A, B and C) to *MNN2* once every 0.5 sec. There is no other traffic. These packets are distributed according to the policies described above. Results are shown in Figure 11.14. The average RTT on the NEMO path over 3G has been 261.9 ms. Changing paths to the NEMO path over the managed Wi-Fi interface, has reduced the RTT to an average of 34.72 ms, which represents an 87% improvement. During the time the ad-hoc mode has been available, the average RTT collected on the OLSR path (ad-hoc link) has been 7.93 ms. In this way, route optimization using MANEMO has further reduced the latency by 26.79 ms, what represents an extra improvement of 77%.

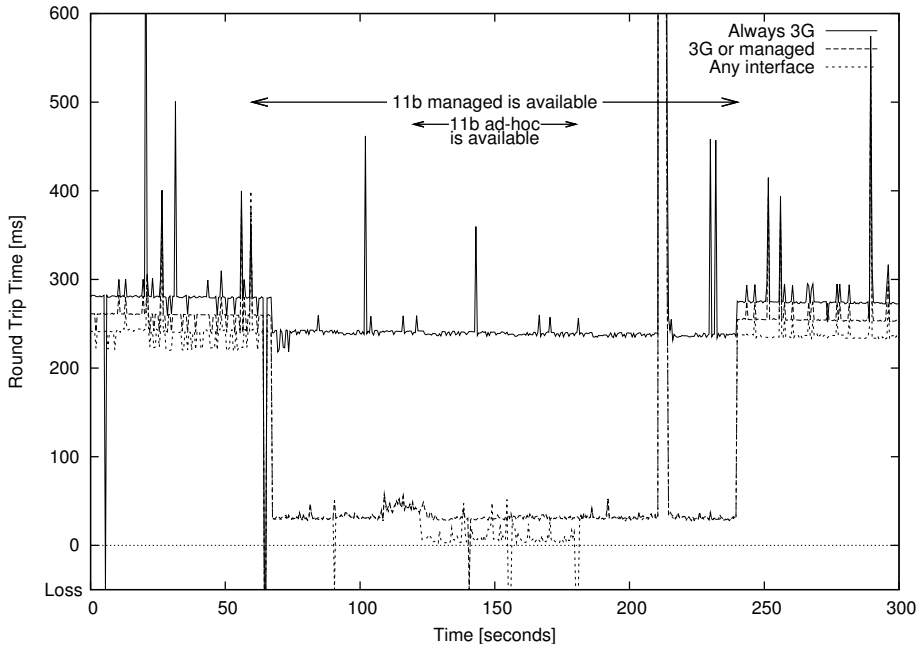


Figure 11.14: Impact of path changes on the RTT, measured using ICMPv6 packets in the absence of background traffic

For the two periods where the three ICMPv6 flows are carried over the 3G network (from $t = 0$ to $t = 60$ and from $t = 240$ to $t = 300$) an offset of 20 ms of delay between them is noticeable. It has been checked that the transmission of the three echo request packets in a consecutive way results in a first-in first-out problem due to transmission and reception

times needed by the 3G driver. The extra overload incurred by the NEMO and tunnel and the Layer-2 Tunneling Protocol (L2TP) tunnel, necessary to support IPv6 traffic in the 3G network, increases the impact of this effect.

Figure 11.15 gives a closer look at the RTT results when the ad-hoc interface goes up/down and paths thus change. At $t = 120$, the ad-hoc interface comes up, and then direct path information of both MNPs are exchanged. At $t = 122.5$, the RTT obtained for the marked packet is 21.27 ms, which comprises an intermediate value between NEMO and OLSR modes. This is because the ICMPv6 echo request has used the NEMO path, while the echo reply has returned through the ad-hoc one. It takes 2.5 seconds for OLSR routing entries to be added to *MR1*'s table after the ad-hoc link has been connected. By contrast, the path is changed back from OLSR to NEMO 1.5 sec after the ad-hoc link is disconnected. During this switching phase, three packets have been lost (From $t = 180$ to $t = 181.5$), due to the sudden disconnection of the ad-hoc interface.

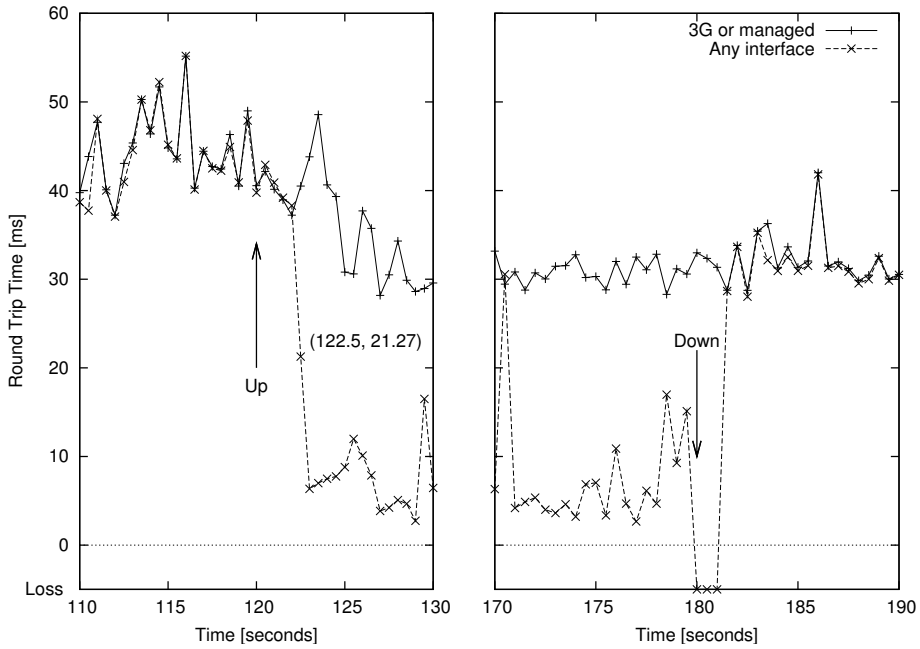


Figure 11.15: Closer look at the RTT values collected when the ad-hoc interface is turned on and off

11.2.2.2 Throughput Measurements

To measure the throughput between MNNs, *MNN1* sends three TCP streams to *MNN2* by means of *iperf*, with destination port numbers 5102, 5101 and 5009, in the same routing scenario used above. At the same time, *MNN1* also sends 56 Bytes ICMPv6 echo request packets as in the previous section. *iperf* gives a report once every two seconds and ping6 gives it every 0.5 seconds. A reference test has been chosen among the set of performed tests. Figure 11.16 shows the achieved throughput with stacked area graph and Figure 11.17 shows the observed RTT when the TCP flows are active.

A summary of throughput results is given in Table 11.6. The average total throughput on the NEMO path over 3G is 455kbps from $t = 0$ to $t = 60$. Since an 802.11b managed network is available from $t = 60$ to $t = 120$, the flows are distributed in two paths and the average

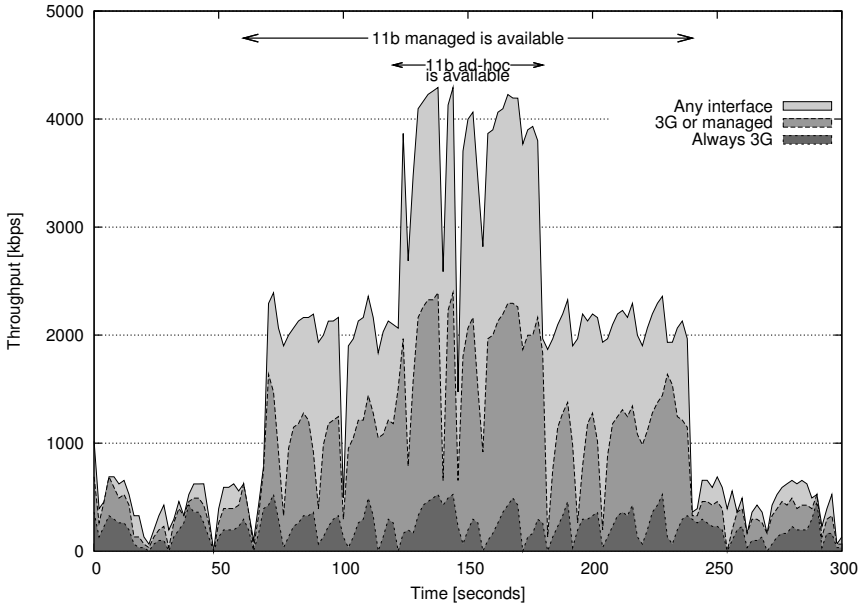


Figure 11.16: Evolution of the throughput of three TCP flows between MNNs using routing policies

throughput increases up to 1913kbps, which represents an improvement of 76% (1458 kbps). From $t = 120$ to $t = 180$, ad-hoc connectivity is also available. The average total throughput increases again up to 3752 kbps when the three TCP flows are distributed through the three paths, which represents a new improvement of 49% (1837 kbps).

The average RTT between MNNs is also listed in Table 11.6. The RTT on the NEMO path is about 400 ms when the three TCP streams are transmitted using the 3G link. When two TCP streams are diverted to the 802.11b managed interface, from $t = 60$ to $t = 120$, the RTT over the 3G link decreases by about 280 ms, which represents an improvement of 30%. The RTT also decreases from 400 ms to about 130 ms for policies "3G or managed" and "Any interface" when Wi-Fi managed is available, which comprises an improvement of 68%. In addition, a further 50% (approx.) of improvement is observed for policies "3G or managed" and "Any interface" when all the interfaces on *MR1* are available, since each communication technology is used by only one flow.

Policy	**Available Interfaces**		
	3G only	**3G and managed**	**All interfaces**
Throughput			
Always 3G	156 kbps	262 kbps	276 kbps
3G or managed	184 kbps	733 kbps	1612 kbps
Any interface	114 kbps	918 kbps	1863 kbps
Total	455 kbps	1913 kbps	3752 kbps
Round-Trip Time			
Always 3G	389 ms	277 ms	275 ms
3G or managed	411 ms	127 ms	64 ms
Any interface	432 ms	130 ms	64 ms

Table 11.6: Total throughput of three TCP flows and RTT between MNNs

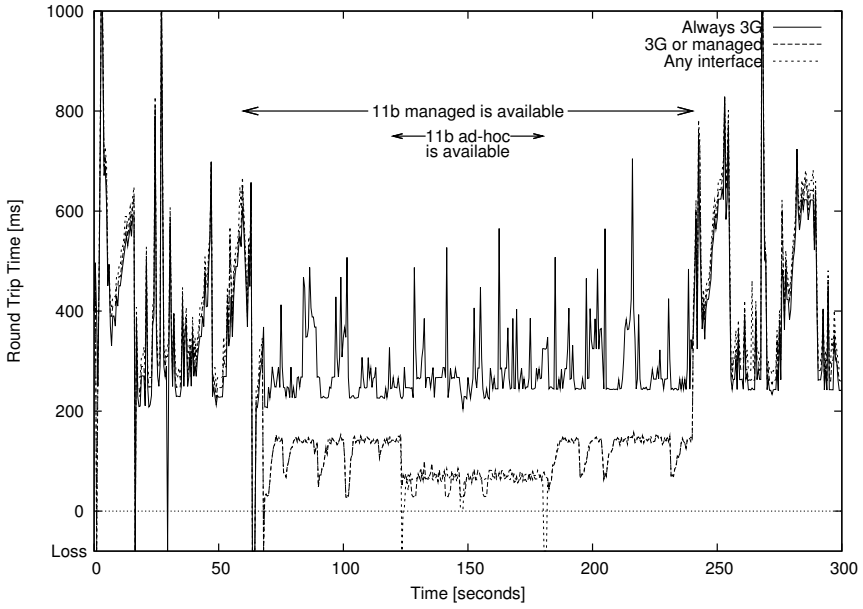


Figure 11.17: RTT between MNNs with three background TCP flows

11.2.3 Field Experiment

The system has been evaluated with a set of field trials performed on the Télécom Bretagne/INRIA Rennes campus. 40 access points have been installed in this area. The test has been performed in a straight road surrounded by buildings, where two access points have been installed at two far away locations. The source vehicle starts moving at a speed of 10 km/h from a position before the first access point, while the destination vehicle with *MR2* has been parked next the two access points. Both MRs were mounted inside the vehicles. Three TCP flows were transmitted from *MNN1* to *MNN2* as in the previous tests. The flow distribution policies of *MR1*, *MR2*, *HA1* and *HA2* are also identical to those of the indoor testbed but, obviously, periods of 802.11 connectivity are not simulated now.

The switch between access media and/or networks has a clear impact on the available bandwidth, as can be seen in Figure 11.18. From $t = 0$ to $t = 60$, the path between MNNs is only via the NEMO path over 3G. The average total throughput of the TCP flows is 344 kbps during this period. The throughput in this field experiment is 111kbps less than in the indoor experiment. This is mostly due to obstacles and movements of the vehicle equipped with *MR1*. From $t = 62$ to $t = 86$ and from $t = 106$ to $t = 116$, the NEMO path through managed Wi-Fi is available, since the moving vehicle is near one access point each time. The average total throughput of the TCP stream at these two periods is 1430.83 kbps and 957.34 kbps, respectively. From $t = 124$ to $t = 130$, the OLSR path over the VANET is available. The average throughput increases until 2408.4kbps during this period.

In the evaluation, the NEMO path on the 802.11b managed interface has been used for 24 seconds for the first access point, and then an additional 10 seconds for the second one. As the speed of the vehicle was 10 km/h, the coverage of the access points can be estimated to be between 30 and 65 meters. The ad-hoc interface has been available during six seconds, thus the VANET range can be estimated to be 17 meters. In this case, the antennas of both MRs were located inside the vehicles. 802.11 performance could therefore be improved by mounting external and/or more powerful antennas.

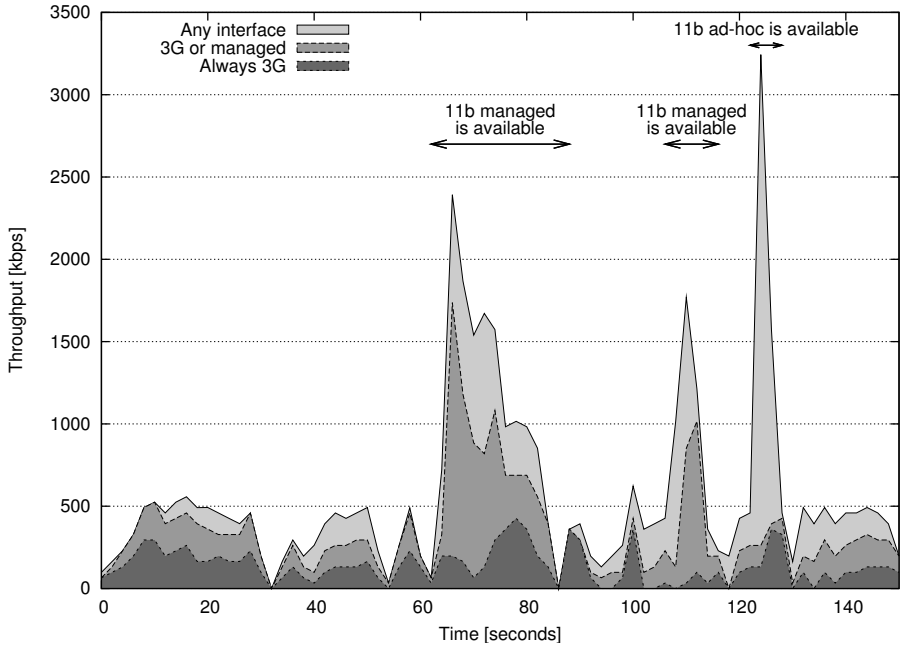


Figure 11.18: Throughputs of three TCP streams in a field experiment. Performances are less stable than in the indoor case

11.2.4 Impact of Geographical Location on Network Performance

In the previous section, the range of the available access points and VANET links are estimated considering a simplification of the driving speed and the time of connection. This section presents more thorough range measurements. These have been collected by maintaining *MR1* (and thus *MNN1*) moving in a 65 meters radius around the position of *MR2*, and reporting the achievable throughputs. None of the MRs has gone out of the access points' coverage and a building sometimes block the VANET path. As the wireless APs are quite close to the test site, the managed interface has been forcibly limited to 1Mbps to account for more distant APs and highlight which network path MR1 uses. By contrast, the ad-hoc interface was not limited and the average throughput between MRs using this interface was 2685 kbps.

The position-mapped throughputs were measured at INRIA Rocquencourt in France, using the GPS-patched version of *iperf*. To obtain a high density of throughput data around *MR2*, the evaluation was actually performed without vehicles. *MR1* has been carried by a human at an average speed of 4 km/h. It starts moving from the position of *MR2* and comes back to the same position within 250 seconds. The experiments were run eight times. All the results are publicly available [3].

A screenshot of the web application can be seen in Figure 11.19. The website displays the throughput between MNNs by varying the size of the blue circles at each measure point. All tests can be displayed by selecting the Log option. Clicking on one of the circles reveals additional information, including the test time, location and offset from the starting point, transferred data size and bandwidth in the last two seconds. All the data can be shown at once with the Show Log button. Users can also analyze the results by changing data density and see the trajectory of *MR1* (and thus *MNN1*).

[3] https://who.rocq.inria.fr/Manabu.Tsukada/experiments/

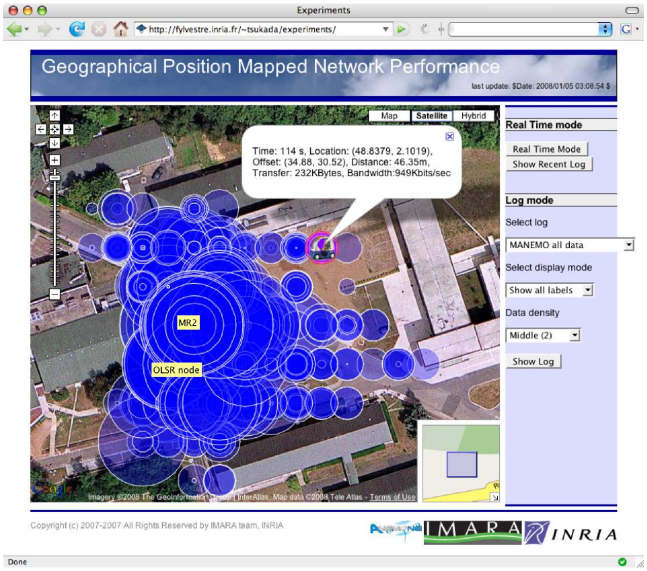


Figure 11.19: Website screen shot of the MANEMO experiment

Throughput results depending on the distance between MNNs can be seen in Figure 11.20. Data points show the throughput obtained at the current distance, while the bar graph represents an average for five meters. Values over 1 Mbps (the arbitrary limitation on the managed Wi-Fi link) are those recorded when the VANET path was available. One can see that it is available up to 40 meters. Between (approx.) 20 and 40 meters, throughput measurements spread over a wide range from 100 kbps to 2700 kbps, because media handovers between the managed and ad-hoc interfaces are performed in these zones.

An asymmetrical tendency of the ad-hoc link ranges has been observed. From the collected results, it turns out that the OLSR path is usable over a longer distance when two vehicles are getting further from one another than when they are getting closer. This hysteresis behavior is due to OLSR's initial delay caused by the period of sharing HELLO packets. This fact is further analyzed in Section 11.1.

11.3 Conclusion

First, Section 11.1 provides a network performance measurement of a VANET maintained by a standard MANET protocol (OLSR) as a benchmark in order to compare with IPv6 GeoNetworking under the same conditions in the next chapter. Then, a proposal to distribute data traffic in vehicular communications combining anchored path (NEMO path) and direct path (OLSR path) has been presented in Section 11.2.

Thanks to AnaVANET, typical statistics are obtained, such as the Packet Delivery Ratio (PDR), Round-Trip Time (RTT), jitter and bandwidth; but also new performance metrics are offered, such as the number of hops used to deliver a packet, or the per-link PDR. Although it has been tuned to dynamic conditions, the OLSR protocol shows limitations to efficiently update routing tables under stressful conditions. This effect is more noticeable when the volume of data traffic is high, due to network overload. The communication is cut when some control messages are lost and OLSR timeouts expire. In all the tests, the line of sight between vehicles has been a key factor to maintain communication links. Moreover, the number of hops used in transmission paths, has been identified as another key performance

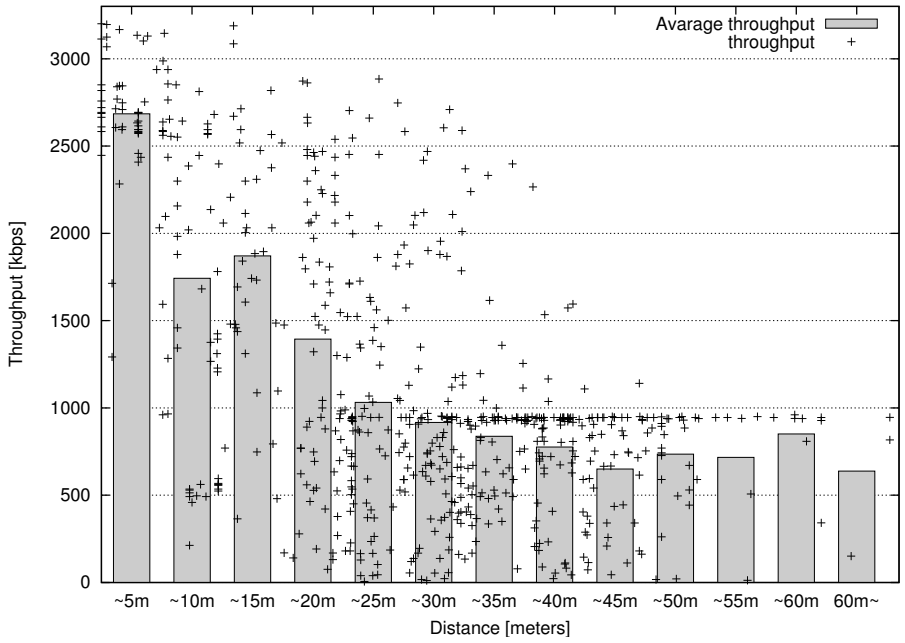


Figure 11.20: Relation between distance and bandwidth using the MANEMO system

factor. An incremental delay between two and three milliseconds per hop has been detected when direct paths between nodes are not used. These cases can be found when the distance between sender and receiver vehicles increase significantly, or when near buildings block the direct communication. However, it has been checked that OLSR prefers smaller paths when communication is possible. The TCP operation over real VANET deployments should be specially taken into account, because the lack of routing information for a while can lead to transport-level disconnection.

The MRs use multiple egress interfaces simultaneously with anchored path (NEMO path) and direct path (OLSR path) in the MANEMO test. The latter could thus mitigate the sub-optimality caused by NEMO paths. Previous experiments results shown that MANEMO with path switching from NEMO to MANET improved network performance in terms of latency and bandwidth. Switching from the a less prioritized path to more prioritized path is performed immediately whereas about two second is needed to switch the other way round, because later requires the detection of unavailability of the primary path. Experimental results show that the achievable throughput and delay are improved when a set of interfaces (3G, 802.11b managed and 802.11b ad-hoc) are available.

More details of this chapter are published in [Tsukada2008, Santa2009b, Santa2009a, Tsukada2010a].

Chapter 12

Evaluation of IPv6 GeoNetworking with GeoNet implementations

Contents

This chapter presents an experimental evaluation of IPv6 GeoNetworking stack implemented by HITACHI and by NEC in the GeoNet project (INRIA involved in the implementation of GeoIP SAP module described in Section 8.5).

We have conducted our experiments on both indoor testbed and outdoor testbed to evaluate the network performance on IPv6 GeoNetworking. The indoor test environment is designed to evaluate the pure performance of IPv6 over GeoNetworking avoiding interferences due to unexpected radio perturbations. We measured the network performance with UDP, TCP and ICMPv6 traffic using *iperf* and *ping6*. Considering the outdoor test, we can see that IPv6 over GeoNetworking works according to the specification in various driving scenarios. The communication is stable even when the vehicle speed is around 100 km/h and when the relative speed between vehicles is high. The radio range is much better than expected. The maximum distance of communication range is around 450 meters and it is not interrupted by the buildings on INRIA campus (all of them has only one floor). This calls for more field tests in urban environments.

12.1 Direct Path Evaluation in Indoor Testbed

12.1.1 ICMPv6 Evaluation

Figures 12.1 and 12.2 show single hop test with GeoNetworking layer implementation with and without next hop cache respectively. Both implementations mark increasing RTT as the packet size increases until the packet size is 1300 bytes which causes packet fragmentation. The packet loss rate is around 5 % on average when no next hop cache is being used, while there is no packet loss when the next hop cache is being used. The difference in the results comes from the fact that one implementation resolves the next hop for every packet via *netlink* as described in Chapter 9.3.1, while the other contains the next hop in the cache for the same IPv6 destination of the packet. This avoids heavy interaction between the userland software and the kernel. With the next hop cache there is a trade-off between reducing the latency of the next hop resolution and having higher possibility to loose the packet in case of a route change. In our tests the next hop cache does not present any disadvantage because the routing entries in the routing table have not been updated during the entire test. For the same reason, the RTT with the next hop cache is 2 ms shorter than the one without for a packet size from 20 bytes to 1300 bytes.

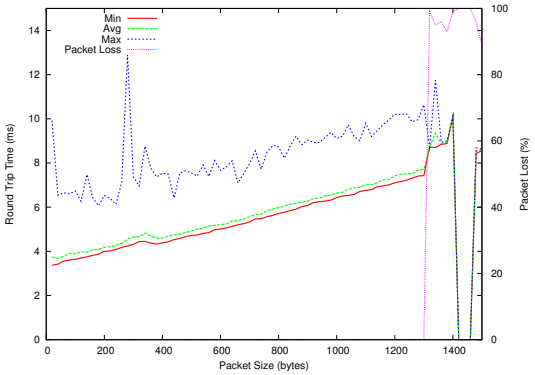


Figure 12.1: HITACHI GeoNetworking layer with next hop cache - single hop

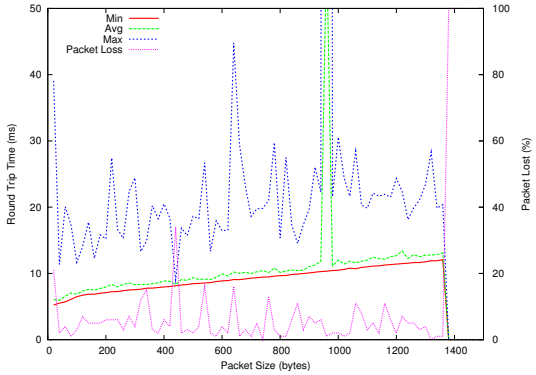


Figure 12.2: NEC GeoNetworking layer without next hop cache - single hop

Figure 12.3 shows the results of the interoperability test where one MR runs HITACHI's GeoNetworking layer and the other one run NEC's. In this test, HITACHI GeoNetworking layer implementation does not resolve the next hop of the IPv6 destination frequently for outbound packets while NEC GeoNetworking layer implementation resolves the next hop for every inbound packet. The RTT is 4 ms with 20 bytes of packet size and 10 ms at 1300 bytes which is almost the average between HITACHI and NEC measurements displayed on Figures 12.1 and Figure 12.2.

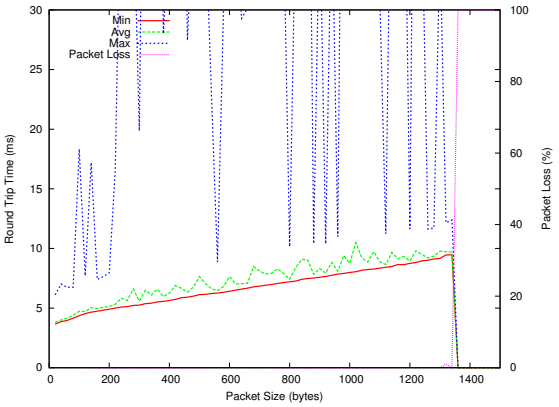


Figure 12.3: Interoperability on single hop

Figures 12.4 and 12.5 show the RTT and packet loss rate in the multi-hop case with GeoNetworking layer implementations with or without next hope cash, respectively. The packet loss rate is under 10% during the test with both implementations. The RTT of both implementations has similar values from 10 ms to 20 ms during the test from 20 bytes to 1300 bytes of packet size. Buffering occurs with the implementation without next hop cache, which causes around 350 ms of delay. As the packets are buffered in the GeoNetworking layer, there is a limited packet loss while RTT is around 350 ms.

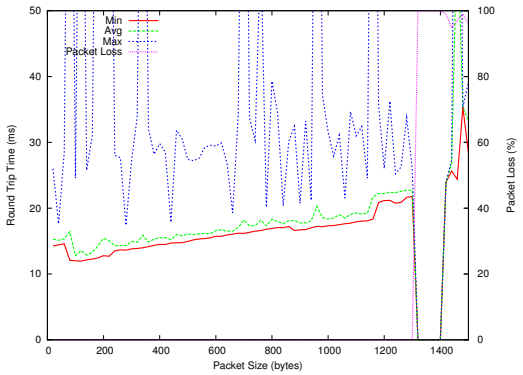


Figure 12.4: HITACHI GeoNetworking layer with next-hop cache - multi-hop

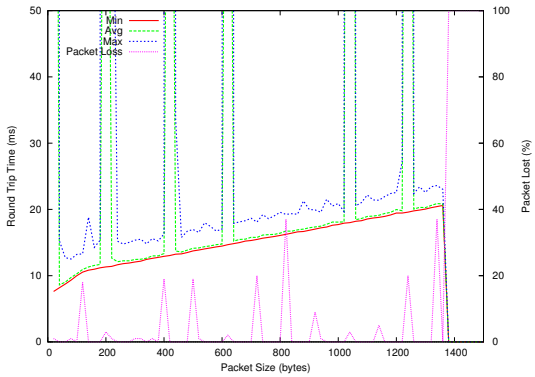


Figure 12.5: NEC GeoNetworking layer without next-hop cache - multi-hop

Figures 12.6 and Figure 12.7 shows the interoperability test between NEC and HITACHI implementations of the GeoNetworking layer. The test is performed with exactly the same configuration as in Figure 12.4 and Figure 12.5 on the source MR and the receiver MR, but

the intermediate MR is replaced by the other implementation. The result shows that the two implementations are fully interoperable.

Figure 12.6 shows the results of the configuration where only NEC implementation is used while Figure 12.5 shows the results of the configuration where HITACHI implementation is used in the middle node. They show almost the same RTT. However the packet loss rate and the packet buffering related delay are significantly reduced.

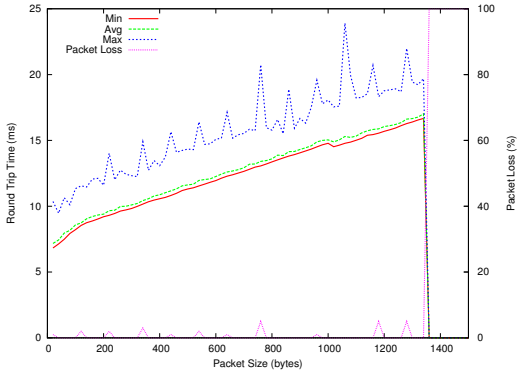


Figure 12.6: NEC-HITACHI-NEC multi-hop

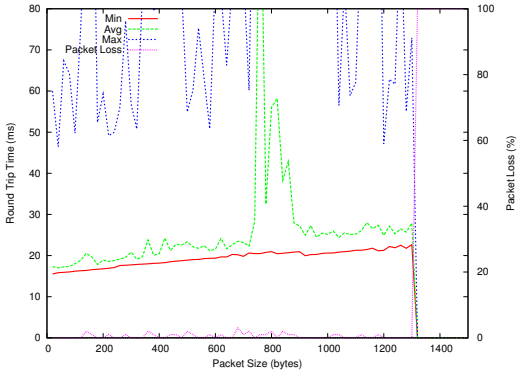


Figure 12.7: HITACHI-NEC-HITACHI multi-hop

Comparison of RTT is given in Figure 12.8. It shows the RTT on single hop without GeoNetworking (red line), single hop with GeoNetworking (green line) and multi-hop with GeoNetworking (blue line). In the single hop case, the RTT with GeoNetworking is 3 ms higher than one without GeoNetworking. In addition, packets with size exceeding 1300 bytes cannot be delivered with GeoNetworking because of the Maximum Transmission Unit (MTU), while the packet without GeoNetworking is delivered until 1500 bytes.

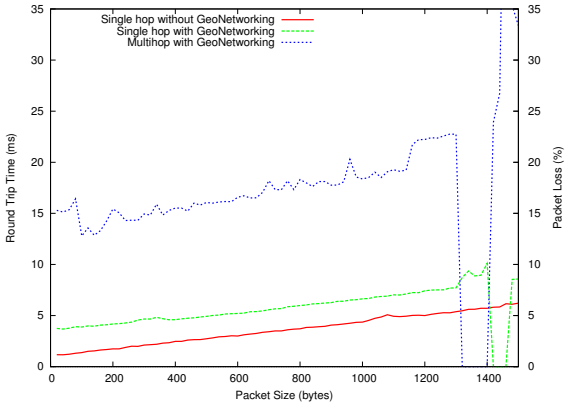


Figure 12.8: Overhead of IPv6 over GeoNetworking

12.1.2 UDP Evaluation

UDP evaluation is performed with various packet sizes ($100 \sim 1900$ bytes) and sending rates ($1M \sim 6M$).

Figure 12.9 shows the PDR on single hop. PDR is low while packet size is small. There is no packet loss with a packet size between 700 bytes and 1300 bytes with 1M of sending rate, between 900 bytes and 1300 bytes of packet size with 2M sending rate and between 1100 bytes and 1300 bytes of packet size with 3M sending rate.

Figure 12.10 shows the throughput for the same tests as reported on Figure 12.9. The throughput is maximized with a 1300 bytes packet size for all sending rates. It shows that the most efficient configuration to send maximum data is realized with a 1300 bytes packet size and 5M sending rate. Maximum throughput is around 4500 Kbits/second.

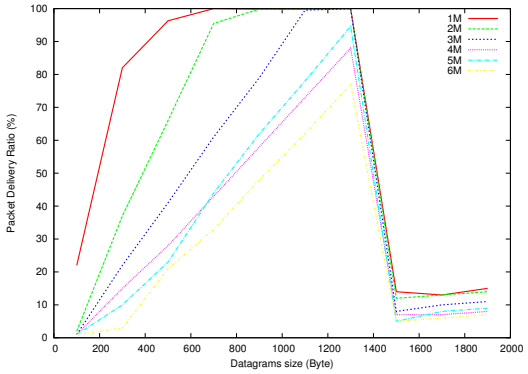


Figure 12.9: Packet delivery ratio - single hop

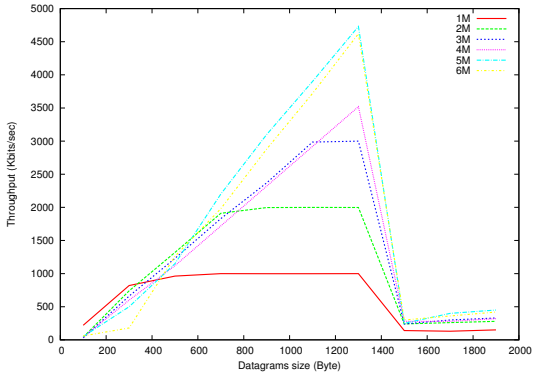


Figure 12.10: Throughput - single hop

Figure 12.11 shows the PDR on the multi-hop path. No configuration allows to reach 100 % PDR. 1300 bytes of packet size is the best configuration to obtain high PDR. More then 90% of packets are dropped under a sending rate above 4M.

Figure 12.12 shows the throughput for the same tests as reported on Figure 12.11. The best throughput is obtained with a 1300 bytes packet size for all the sending rates. The best configuration on the multi-hop path is 1300 bytes of packet size and 2M of sending rate that is reached around 1400 Kbits/ second.

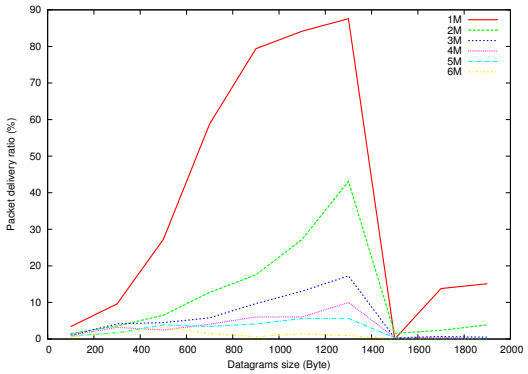


Figure 12.11: Packet delivery ratio - multi-hop

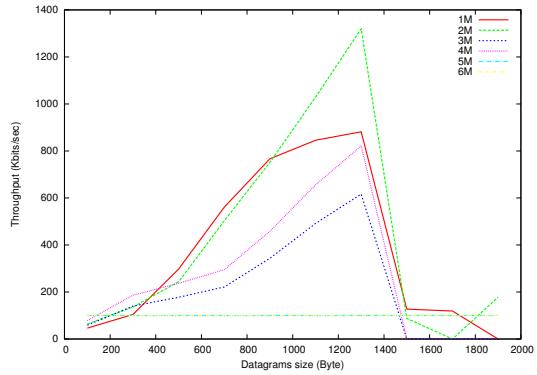


Figure 12.12: Throughput - multi-hop

12.1.3 TCP Evaluation

We observed that TCP transmission does not work well with the current implementation of IPv6 over GeoNetworking. The throughput on the single hop path with HITACHI GeoNetworking implementation is shown in Figure 12.13 and the throughput on the multi-hop path on HITACHI is shown in Figure 12.14. Figure 12.10 shows that the throughput of TCP on the single hop path is under 200 Kbits/second which is extremely low compare to UDP tests reported in the previous section. Figure 12.12 also shows that the throughput of TCP on the multi-hop path is low (under 85 Kbits /second).

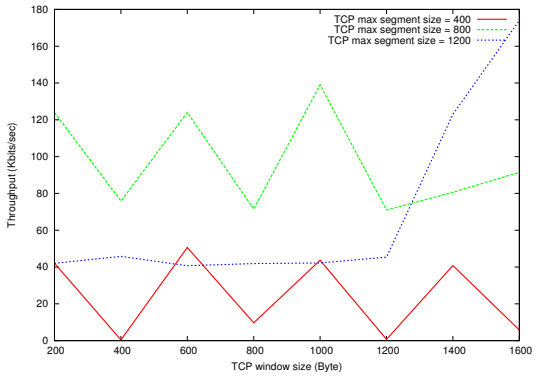


Figure 12.13: Single Hop Throughput with HITACHI

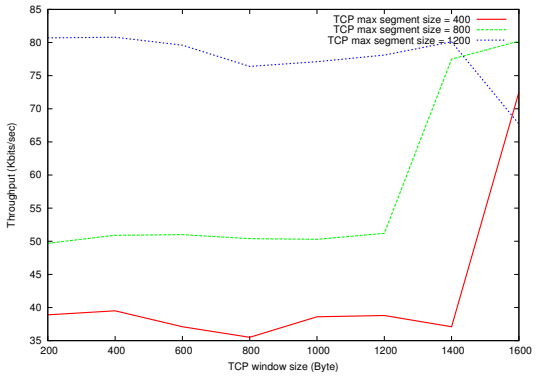


Figure 12.14: Multi-hop Throughput with HITACHI

We investigated this problem deeper with *tcpdump* logging. The log is taken in the static test described in Section 11.1.3. In the static test, we could check that the multi-hop configuration works in both unidirectional and bidirectional ways, meaning that UDP works with good quality (about 10 % packet loss), and ICMPv6 works without problems. According to the *tcpdump* result, the problem comes from the collision between the input and output traffic on the tun0 interface, which is the implemented interface between the GeoNetworking and IPv6 layers. In the TCP traffic case, some data simultaneously arrives in both ways (from GeoNetworking to IPv6 and from IPv6 to GeoNetworking). Some data is lost in the collision and the TCP connection is broken by these dropped packets.

12.2 Anchored Path Evaluation in Indoor Testbed

The latency and PDR evaluation of the anchored path is performed using the indoor testbed with the network configuration described in Section 10.6.2. The source MR connect to the AR with multi-hop communication (two hop) as in Figure 10.6. We used the HITACHI implementation for these evaluations.

12.2.1 Latency evaluation

To evaluate the latency, we measured the RTT between the two end-points. The MNN sends ICPMv6 Request every 0.1 second. The ICMPv6 packet is increased by 20 bytes. The packet size is varying from 20 bytes to 1500 bytes. From the obtained results, we extract the maximum, the minimum and the average RTT as well as the packet loss for each packet size.

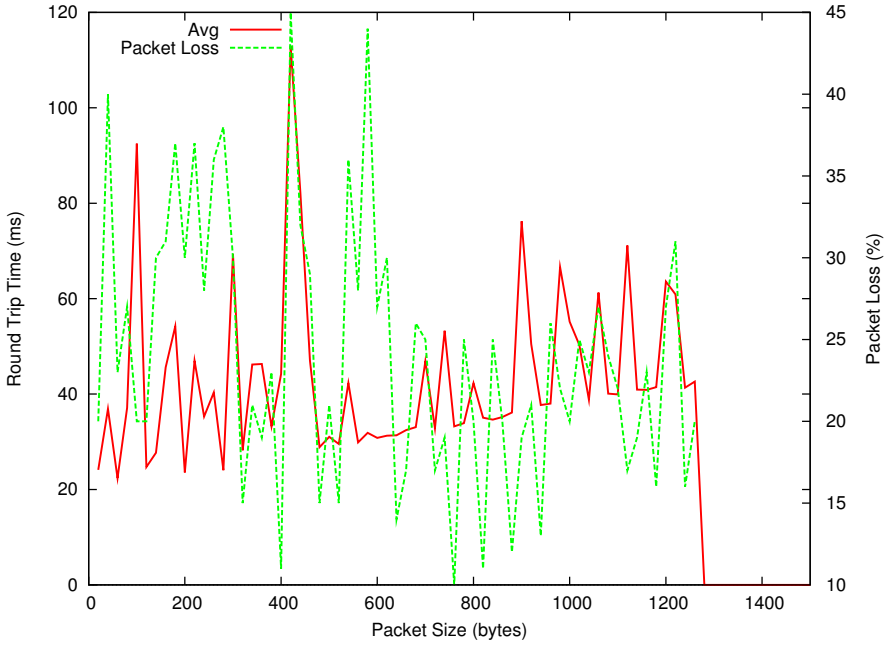


Figure 12.15: RTT between MNN and CN

As depicted in Figure 12.15, we evaluate the average RTT between the CN and the GeoNet MR and the packet loss. The maximum RTT is around 110 ms which corresponds to the maximum packet loss (45 percent) for 420 bytes of packet size. As we can see in Figure 12.15, packets with size exceeding 1300 bytes cannot be delivered by GeoNetworking due to the MTU of the packet. At the time of writing this paper, the packet fragmentation operation was not yet implemented in the GeoNetworking layer.

12.2.2 Packet delivery ratio evaluation

In this tests, we evaluate the packet loss ratio in a UDP communication. The packet delivery ratio is the percentage of packets arriving at the receiver divided by the packets sent by the sender. The UDP packets are generated in the MNN attached to the MR, sent through the GeoNetworking link to the HA and finally to the CN. The sender sends UDP packets to the receiver with fixed rate. The UDP client and server save the log file traces. After the tests, the log files of both the client and the server are parsed through pointers (the port number) and the packet loss results are plotted. In these tests, the bandwidth is varying from 1 to 6 Mb/s. For each bandwidth value, the read-write buffer is increased from 20 bytes to 1900 bytes. The throughput is shown on the receiver side. As illustrated in Figure 12.16, when the packet has a small size, the packet delivery ratio is weak. The best values are obtained when the packet size is between 800 and 1300 bytes for the lowest sending rate; when the bandwidth is 1 M and the packet size is 1300 bytes, the packet delivery ratio is almost 100 percent. The maximum throughput is around 2500 Kbits/second. It reaches its maximum when the packet size is 1300 bytes packet. It corresponds to a 5M sending rate.

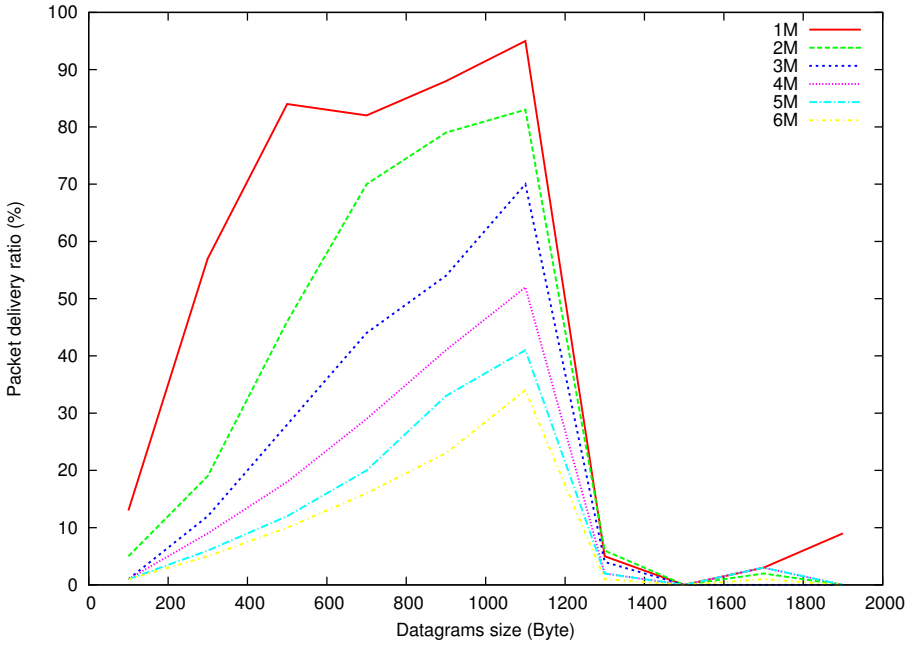


Figure 12.16: Packet delivery ratio between MNN and CN

12.3 Direct Path Evaluation in Real field Testbed

12.3.1 Distance Test

The evaluation of the distance has been performed with two cars considering the distance test as described in Section 10.7.1. The sender vehicle gets away from the receiver vehicle (whose position is static), and then comes back when the communication is interrupted, and finally returns to the initial point. The speed of the sender was maintained less than 10 Km/h to smoothly check the loss of connectivity.

Figure 12.17 shows the RTT with ICMPv6 transmission. The RTT is within 5 ms to 10 ms until 420 meters. After this point, no packets are delivered, until the sender vehicle comes back and reaches 100 meters of distance. Since periodical GeoNetworking beacon messages are lost when the distance is around 420 meters, the destination GeoNetworking ID is removed from the location table and the transmission ends at this point. It takes 50 seconds to come back to a distance of 100 meters where ICMPv6 recovered during previous test.

Throughput using TCP and considering the same scenario is given in Figure 12.18. The maximum throughput is around 1000 Kbits/sec when the vehicles are parked next to one another. When the distance is from 50 meters to 200 meters, the average throughput is around 500 Kbits/sec and the TCP communication is interrupted at 270 meters. The communication does not recover during the rest of the test, because the TCP session time out.

The PDR using UDP with the distance test is shown in Figure 12.19. The PDR is almost 100 % from beginning to 200 meters. From 200 meters, the packets are starting to be dropped and the packet transmission finally ends at a distance of 420 meters. The packets are not delivered until the vehicle comes back to a distance of 400 meters 50 seconds after the communication ends.

The jitter of in the same test is illustrated on Figure 12.20. When the sender car leaves

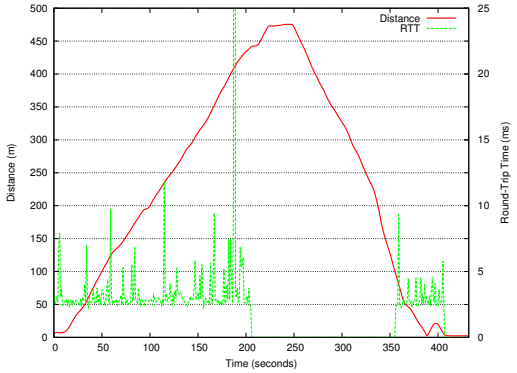


Figure 12.17: RTT on ICMPv6 with distance

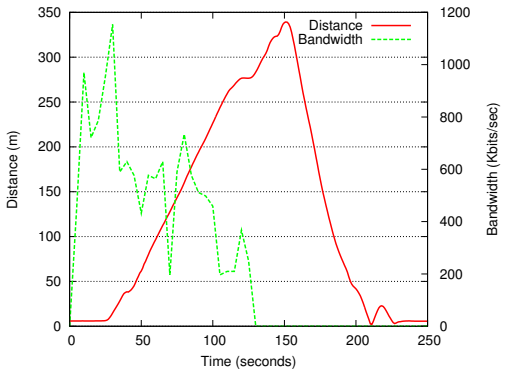


Figure 12.18: Throughput on TCP with distance

the receiver one, at a distance between 250 and 420 meters, the jitter is higher, due to layer two retransmissions caused by the increase of the distance. When the sender approaches the receiver again, this effect, but higher, is again visible at distances between 400 and 200 meters. This is due to packet flood of buffered packet during the disconnected period.

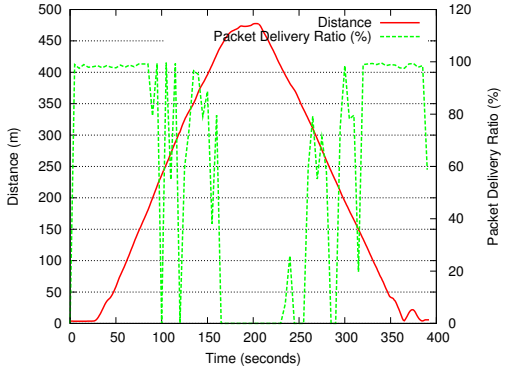


Figure 12.19: packet delivery ratio on UDP with distance

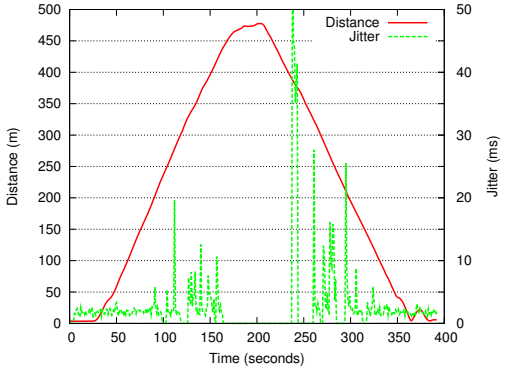


Figure 12.20: Jitter on UDP with distance

12.3.2 Static Test

The results of Static test (three parked vehicles, see Section 10.7.2) are summarized in Table 12.1. The total distance between the sender and receiver vehicles was 330 meters (220 plus 110 meters). The average PDR and throughput were 90.18% and 901.95 Kbits/sec. As expected, the packets were sometimes transmitted directly from sender to receiver. It was foreseeable because there are large obstacles (buildings) near the receiver and the sender. And the PDR degrades to 21.88 % at the path change. The jitter reached up to 39.2 ms at during path change period while the average jitter is 2.98 ms. The PDR was stable around 95%.

The RTT with ICMPv6 packet is also summarized in Table 12.1. The communication is unstable during 300 seconds. The RTT varies from 4.6 ms to over 5000 ms. This is due to

the link failure. 600 ICMPv6 packets are sent during the test (2 packets in a second). The packets passed via four links when the communication goes over the multi-hop path. We see the packet loss in all the links. 31 packets are dropped on the first link, 18 packets on the second link, and 65 packets on the third link and 10 packets on the last link. The total packet loss was 124 packets which represent 20 % loss. Also 4 packets went on a single hop path and 9 packets went on an asymmetric path. There was a stable period of 25 seconds during which packets always went through a multi-hop path. During this period, the average RTT was 5.81 ms as for the indoor tests analyzed in Section 10.6.

Test	Metric	Minimum	Average	Maximum	Standard deviation
UDP 3 vehicles	PDR(%)	21.88	90.18	98.13	14.99
	Bandwidth (Kbps)	274.56	901.95	998.4	151.31
	Jitter (ms)	1.25	2.89	39.2	5.27
ICMPv6 3 vehicles	RTT(ms) all 300 sec	4.6	477.43	5080	992.31
	RTT(ms) stable 25 sec	4.74	5.81	9.66	1.46

Table 12.1: Network Performance in static test

12.3.3 Urban Test

This evaluation has been performed with three cars considering the urban test as described in Section 10.7.3. According to the scenario, three vehicles have been driven around a set of buildings, with the intention of blocking the direct link between Vehicles 3 and 1. The speed of the test where set between 15 km/h and 30 km/h. Figure 12.21 shows the RTT and hop count with distance between *MR1-MR2* and *MR2- MR3*.

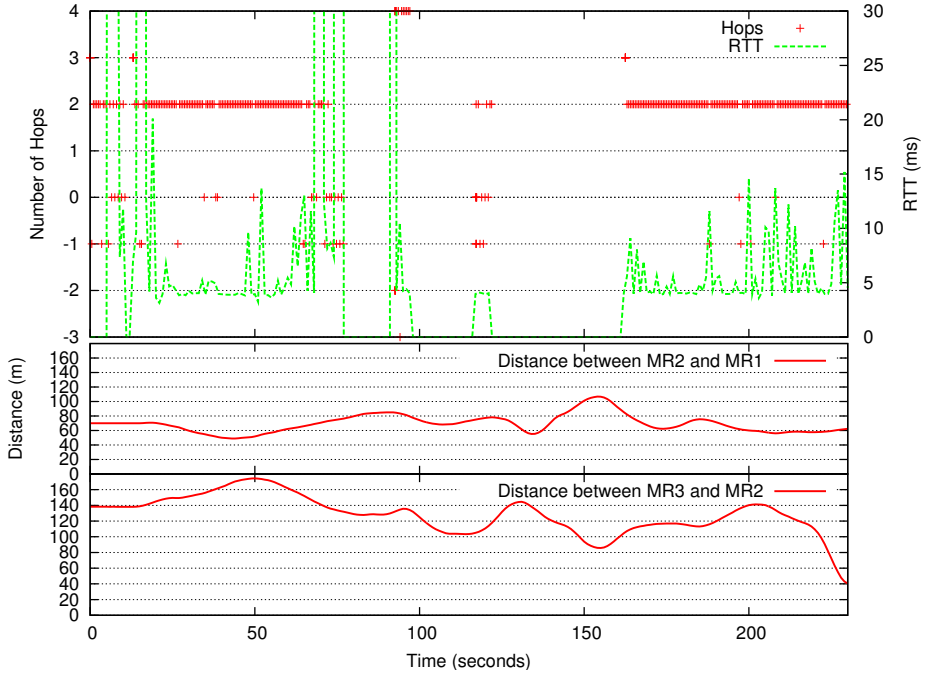


Figure 12.21: RTT and hop count with distance (under 30km/h)

The two-hop and four-hop cases are corresponding respectively to bidirectional single hop and multi-hop paths (ICMPv6 echo request and echo reply take the same path). Several three-hop routes have been monitored, due to, sometimes, the ICMPv6 Echo Request packets taking a different route than the Echo Reply ones. At some period, no hop count is marked because the sender MR does not send any packet due to lack of next hop GeoNetworking ID in the location table because it beacons were not received. In this case, no packet is emitted from the MR. In the test, most of the packet transmission passed to single hop (two hop for returning); this is because the GeoNetworking layer tries to select each hop as distant as possible in order to minimize the hop-count. The mechanism works very well and the INRIA Rocquencourt (500 meters × 250 meters) campus is too small to observe multi-hop path.

Figure 12.22 shows hop count, PDR and jitter on dynamic tests less than 30 km/h.

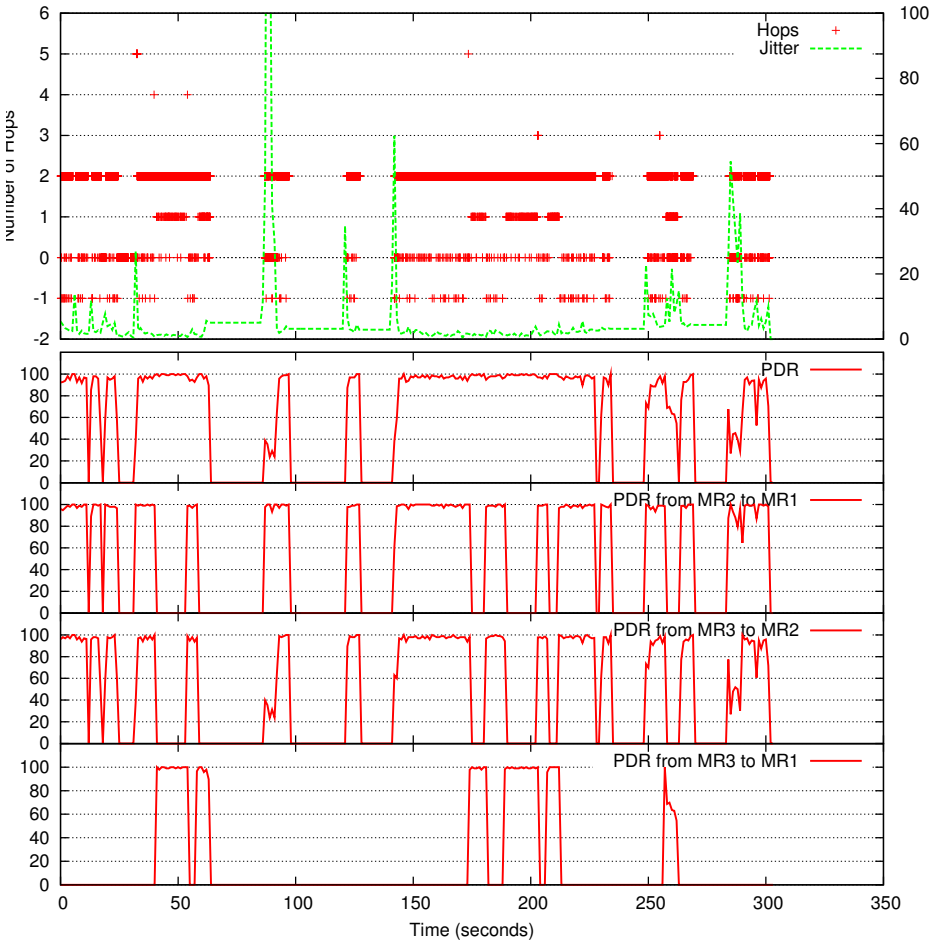


Figure 12.22: Hops, Packet Delivery Ratio and jitter on dynamic test

The upper plot shows the number of hops used in the paths followed by UDP packets, whereas the lower graphs show the PDR, computed end to end and per link. The PDR is calculated per second, while the hop-count is plotted for each packet transmitted from the sender node. When no hops are drawn, the route to the destination vehicle is not available. Zero hops means that the packet was sent by the first MR but was not received by any other. Negative values represent those packets which did not arrive to the destination vehicle, but some hops were reached. As can be seen, a direct relation exists between PDR and number

of hops. When this last value is equal or lower than zero, the PDR decreases. When the vehicles are in the same street, some direct paths (one-hop) appear; however, when the distance between the sender and the receiver vehicles is large enough, the two-hop route is used. These different types of paths can be also seen if the per-link PDR is observed. Whereas the direct link (*MR3-MR1*) gives intermediate PDR values, the PDR between consecutive vehicles is almost identical and near 100% when the two-hop link is used, due to the lower distance between nodes.

12.3.4 Highway Test

The dynamic tests performed over highway conditions as described in Section 10.7.4. The speed of the cars was around 100 km/h, but the distance between vehicles was variable, due to the rest of traffic on the road. Moreover, communication problems in this test are not only due to buildings, but also to surrounding vehicles. Figures 12.23 and 12.24 show hop count and RTT with distance between *MR3-MR2* and *MR2-MR1*. And the relation between the distance between 3 cars, PDR, and hop count is shown in Figure 12.25

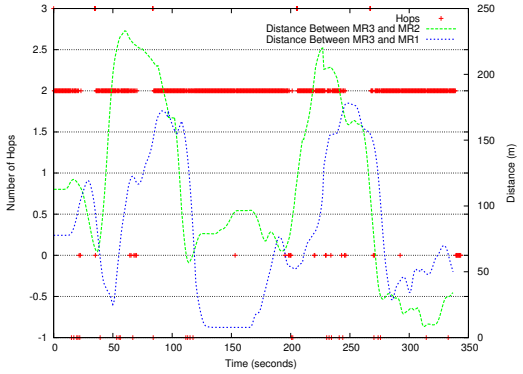


Figure 12.23: Hops with distance on dynamic test

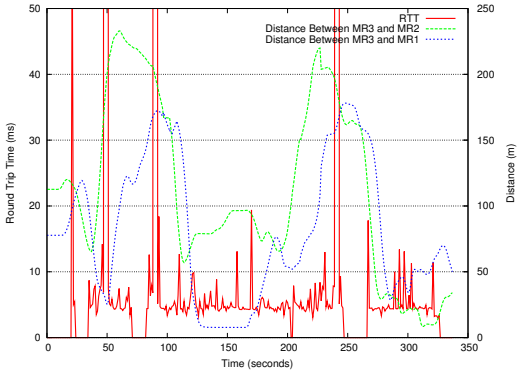


Figure 12.24: RTT with distance on dynamic test

12.4 Conclusion

Indoor test shows that the two implementations of GeoNetworking made by HITACHI and NEC are perfectly interoperable. The experimental results show that IPv6 over GeoNetworking does not have too much delay (less than 4ms on a single hop and less than 15 ms on a three hops) and is feasible for vehicle communication. The delay on a single hop and multi-hop is improved by two optimization works in addition to GeoNet specifications. First, the next hop IPv6 address cache is implemented to reduces the overhead from the next hop IPv6 address resolution on the Geo-IP SAP that causes overhead in term of delay. Second optimization is using multi-hop beaconing so that the source MR obtains the destination MR's position multi-hop away proactively instead of demanding it with reactive way (location service). However, the first optimization has a trade-off between reducing the latency of the next hop resolution and packet loss probability in the case of path change. The second optimization also has a typical trade-off between proactive and reactive mode of MANET depending on the communication scenarios as described in Section 3.3.1. We need to investigate

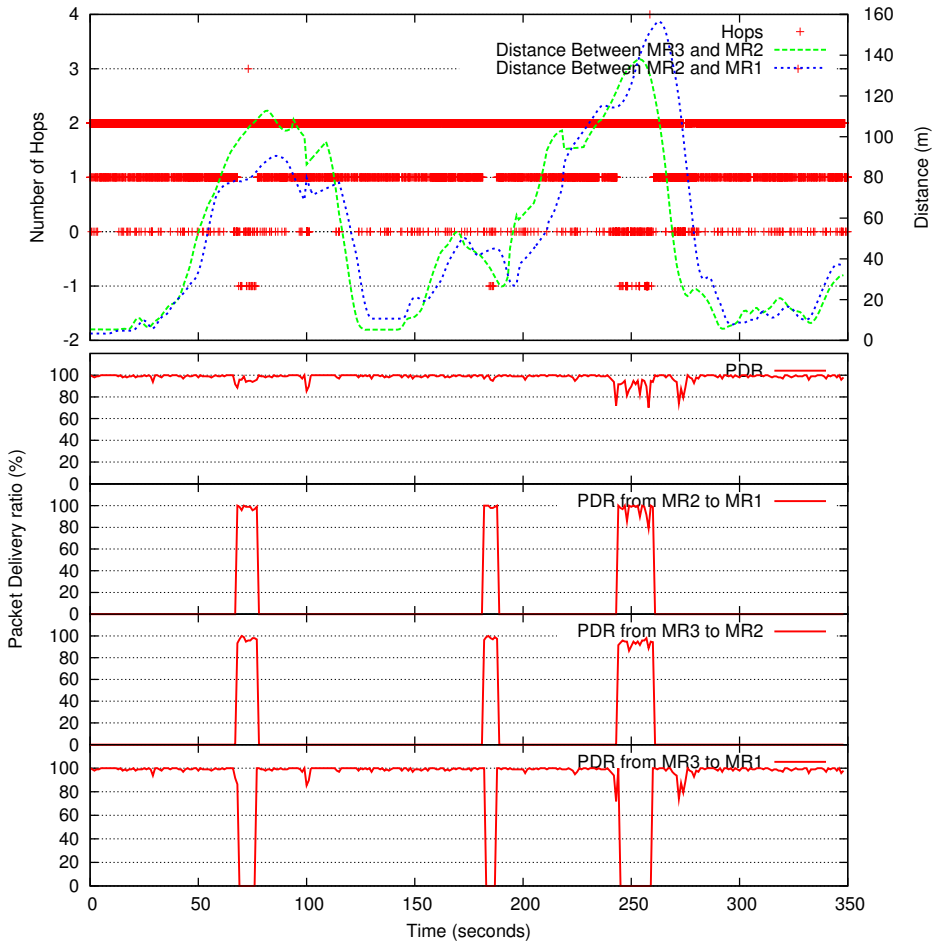


Figure 12.25: Hops and packet delivery ratio with distance on dynamic test

the trade-off in the future.

Network performance in term of delay and Packet Delivery Ratio (PDR) are not degraded by NEMO over GeoNetworking. We conclude there are no much bad influence from the NEMO header. The other typical causes of NEMO performance degradation such as network traffic congestion on the HA when the HA serves many MR and additional hops by forcing the packet to the HA are not observed, because we have no other MR generates network traffic nor much additional hops since the HA is located in a few hop away from the MR and the CsN. These affect have to be investigated as future works.

Our outdoor tests show that the performance of the implementations under multi-hop scenarios must be improved. Under the conditions of our limited vehicular scenario, hardware and the implementations, a number of 3 hops and distance around 1500m between the vehicle and the roadside seems to be a limit. This calls for more scientific work to determine the appropriate radius of the geographic link for GeoBroadcasting IPv6 Router Advertisements. TCP doesn't work well with the current implementation because of packet loss by the collision of input and output at the level of the Geo-IP SAP (UDP works because it is one way communication and ICMPv6 works in both ways because packet interval is high).

More details of this chapter are published in [GeoNet-D.7, Tsukada2010b, Ines2010].

Chapter 13

Evaluation of IPv6 GeoNetworking with CarGeo6 implementation

Contents

In this chapter, we describe the evaluation results of performance measurement of the CarGeo6 implementation, by means of experimental evaluation in indoor testbed and outdoor testbed. The basic configuration of the evaluation is common with the test performed in the previous chapter using the GeoNet implementations. Thus we compare the performance difference between them. With outdoor testbed, we evaluate the performance in Internet-based communication by combining CarGeo6 and NEMO implementation (MIP6D). The performance measurement are processed and analyzed with AnaVANET.

More details of indoor tests are published in [Toukabri2011].

13.1 Direct Path Evaluation in Indoor Testbed

The latency is evaluated by the RTT value indicated in the ping6 output. The ping6 output indicates the minimum, maximum and average RTT for a given size of packet. The test consists on sending 100 ICMPv6 requests every 0.1ms with different packet size values increased each time by 20Bytes and varying from 20Bytes to 1500Bytes. The ping6 output indicates also the packet loss average for each size of ICMPv6 packet. We report in Figure 13.1 and Figure 13.2 the results we had for a ping6 from MNN1 to MNN2 in both single hop and multi-hop configurations.

13.1.1 ICMPv6 Evaluation in Single hop scenario

Figure 13.1 indicates first that there is packet loss for a packet size exceeding 1300Bytes. This is explained by the fact that we fixed the MTU of the TUN/TAP virtual interface to 1350Bytes in our test, which means that packets from 1320Bytes and more are automatically dropped as no fragmentation mechanism is neither enabled nor implemented at the TUN/-TAP interface. The lack of a fragmentation mechanism at the GeoNetworking layer could also have an impact on the packet loss: The maximum MTU is fixed to 1500Bytes. The figure shows also that the average RTT for all packet size values varies mostly between 2ms and 10ms except for a packet size of 370Bytes where we noticed a 25ms maximum average RTT value with 8% packet loss.

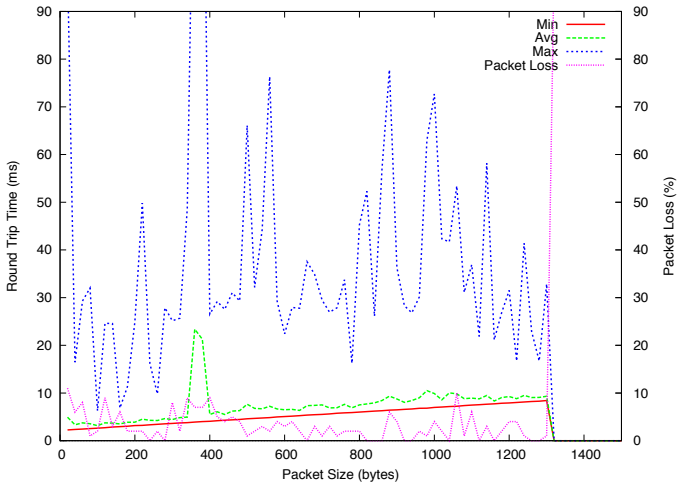


Figure 13.1: ICMPv6 performance in single hop case

If we compare these results to GeoNet results described in Chapter 12 for the same test,

we can say that CarGeo6 average RTT values are globally better than GeoNet average RTT. Same as for the packet loss, values are almost similar in both implementations. However, these results could be improved by the implementation of an IP Next Hop cache. Currently, the IP Next Hop is resolved for each IPv6 packet at the IPv6 over GeoNetworking sub-module (adaptation module) which implies a processing delay on the RTT. The IP Next Hop cache avoids the software resolving the IP Next Hop address for packets having the same destination address. In other words, the cache will keep in a periodically refreshed table the destination GeoNetworking ID of an IP Next Hop and will not repeat this operation for packets having the same destination.

Besides, the packet loss values (maximum of 11%) could also be improved. Even if the indoor testbed is intended to minimize interferences impact on the experiment, we cannot suppress definitely this constrain that could be caused by wireless engines located in the proximity of the testbed. Thus, interference impact could be avoided by the choice of a less noisy wireless channel and the isolation of the testbed as well as possible. The activation of QoS at the wireless interface could also improve the packet loss but may imply unfortunately an overhead.

13.1.2 ICMPv6 Evaluation in Multi hop scenario

As depicted in Figure 13.2, we can see that global values of RTT and packet loss are significantly higher with one GeoNetworking Forwarder node than in the single hop configuration. The minimum packet loss value is 40% for a 1340Bytes packet size. Moreover, as in single hop case, packets are lost for packet size values over 1350Bytes due to the lack of fragmentation mechanisms at the GeoNetworking layer. The maximum average RTT is also noticed for a 370Bytes packet size. Globally, RTT values in multi-hop are about 10 times higher than RTT values in single hop case and more than 40% packets are lost.

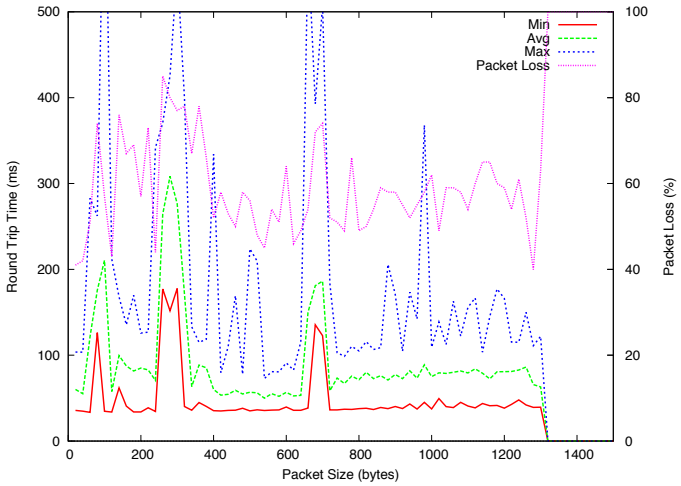


Figure 13.2: ICMPv6 performance in multi-hop case

As written before, RTT values could generally be improved by the implementation of an IP Next Hop cache but we assume that this is not sufficient in the multi-hop case. RTT and packet loss high values are caused also by the Location Service mechanism implemented at the GeoNetworking level. This mechanism is responsible for finding the GeoNetworking ID of a node not in the neighborhood of the source. A process of Request/Reply packets

is then triggered in order to find that ID. This mechanism implies a lot of waiting time until the source gets the reply with the GeoNetworking ID of the destination: the more we have intermediary nodes the bigger is the RTT and chances of packet loss. To improve this, a multi-hop beaconing mechanism where the source beacon is relayed until the destination through intermediary GeoNetworking forwarders could be added.

13.1.3 Overhead of IPv6 GeoNetworking in ICMPv6 Evaluation

In order to evaluate the overhead between IPv6 and GeoNetworking, we compare in Figure 13.3 the RTT values for different packet size for IPv6 without GeoNetworking and for IPv6 with GeoNetworking. The figure shows that the overhead between IPv6 and GeoNetworking in the single hop case is about 3ms, while it reaches 30ms in the multi-hop case. We think that this overhead (multi-hop case) could be reduced if we implement the multi-hop beaconing mechanism instead of the Location Service mechanism.

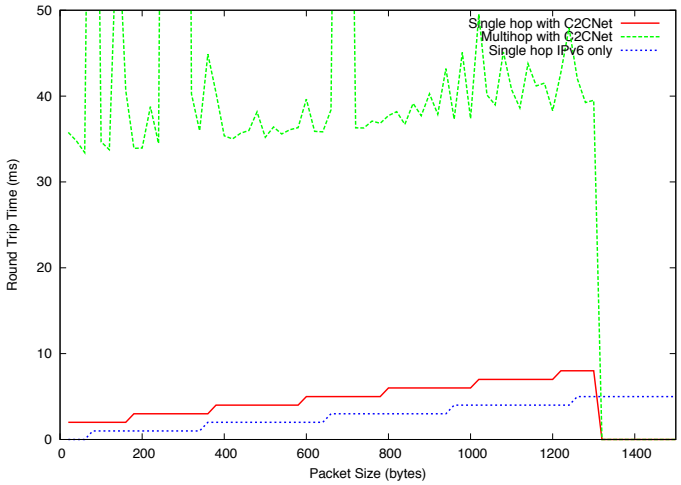


Figure 13.3: Overhead between GeoNetworking and IPv6

13.1.4 UDP Evaluation

In this part, we report UDP performance results for the single hop case. The performance is evaluated according to packet delivery ratio values and the throughput at the receiver side. The test consists on varying the datagram size from 100Bytes to 1900Bytes for different values of the UDP sending rate varying from 250Kbits/sec to 2Mbits/sec.

Figure 13.4 shows the packet delivery ratio in the single hop case. The packet delivery ratio is low when the datagram size is too small: 60% packets are delivered for a 700Bytes datagram size and 250Kbits/sec sending rate. The maximum packet delivery values (97% to 100%) are registered for a datagram size between 1150Bytes and 1380Bytes and with 250Kbits/sec sending rate. Though, only 50% packet delivery is registered for these same datagram sizes with 1Mbits/sec sending rate.

Figure 13.5 shows the throughput delivered in the same test. Throughput is maximized for all rates with ~1360Bytes datagram size. Besides, the maximum throughput value is registered for 420Bytes datagram size with 1250Kbits/sec, 1750Kbits/sec and 2Mbits/sec sending rates. We decided to limit our measurement interval to 2Mbits/sec sending rate because packets are dropped for rates more than this value.

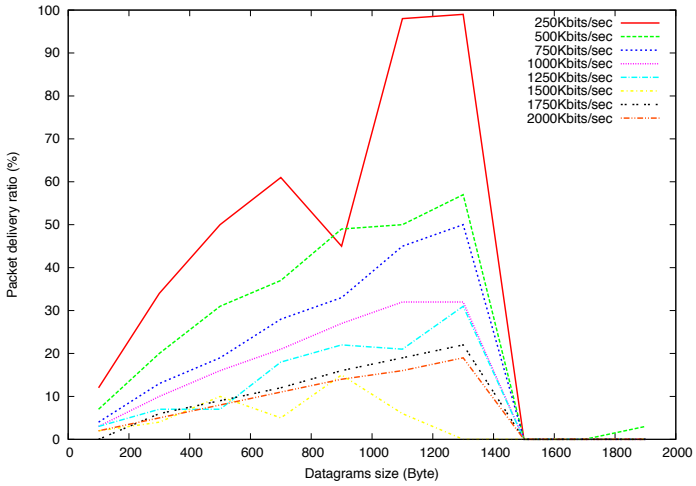


Figure 13.4: UDP performance in single hop case

In comparison with GeoNet results for UDP performance described in Chapter 12, CarGeo6's performance for UDP is currently poor but could be improved. Possible reasons for this results could be first wireless media issues due to interference as mentioned before.

Besides, the quality of the GeoNetworking link could also be the issue. As we suspect processing delays at the GeoNetworking layer, this could have an impact on the UDP traffic transmission from the source to the destination.

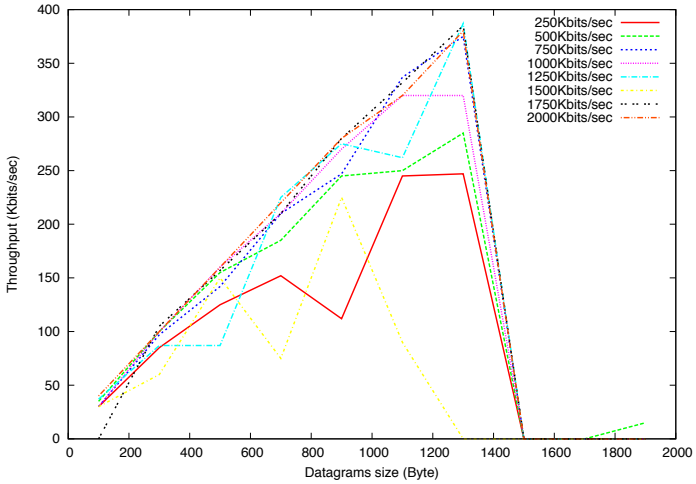


Figure 13.5: UDP throughput in single hop case

Currently, our assumption is the following: With the *iperf* tool, the server sends statistic information about the link state to the client (sender node) periodically after receiving a certain number of datagrams. If packets take too much time to arrive, and as UDP is an unreliable protocol, the server could send state information of the link before receiving the packets. This means that late arrived packets could be considered as lost. Moreover, we noticed according to the Figure that, the bigger the sending rate is, the lesser packets arrive to the destination. This could confirm the assumption that the processing time implies too much delay on the communication: the bigger the packet is, the bigger the processing delay

will be, and the bigger the chance to lost the packet is.

13.2 Anchored Path Evaluation in Real Field Testbed

13.2.1 Handover Scenario

ICMPv6 and UDP evaluations in handover scenarios were performed in INRIA Paris-Rocquencourt campus with two ARs. The two ARs are installed in different buildings as shown in the maps in Figure 13.6 and Figure 13.8. The software and hardware configuration of the two ARs are identical to the MR used in the previous section. Otherwise, the ARs sends RA in the GeoNetworking link with 3 seconds interval. The ARs do not have GPS device, and instead of that, the position is pre-configured statically. Without GPS, the method to synchronize the hardware time to GPS (See Section 10.8.2 for details) for AnaVANET is not available in the ARs. Instead of using GPS, Network Time Protocol (NTP) is used. For administrative reason to allocate new prefix to AR2, IPv6-to-IPv6 tunnel are established from the Ethernet of AR2 to the router next hop to the HA used in the tests. This configuration gives 40 bytes of additional header to the packets, but it does not incur any additional hop of router on the route of the packets.

As shown in the itinerary in Figure 13.6 and Figure 13.8, AR2 is only available in the most time in the tests and AR1 is available in the last. Thus we could expect handover at the last of the test. This is because the building behind AR1 blocks the line of sight to the square that the vehicle goes around. And also, the building stands on the corner in north west of the square blocks the wireless radio to AR2. Approximately ten trees in the south of the square can be obstacles to the access to AR2.

The speed of the vehicle was limited to less than 15 km/h like in urban scenario. The MR equipped in the vehicle has same hardware configuration appears in the previous sections. The speed of the vehicle was limited to less than 15 km/h like in urban scenario. The MR equipped in the vehicle has same hardware configuration. The modified MIP6D described in Section 9.4 is installed to the MR. The HA supports the AR locates in INRIA campus and the lifetime of the binding are configured as 12 seconds. The CN also locates in INRIA campus, and from the MNN connected in the vehicle to the CN, the traffic of ICMPv6 and UDP are generated by *ping6* and *iperf* software.

All the result of the real field evaluations are also published in the website[1].

13.2.2 ICMP Evaluation in Handover Scenario

In the scenario shown in Section 13.2.1, ICMPv6 echo request (64 bytes) is sent from the MNN to the CN twice in a second. The CN replies the echo reply. The results collected in the ICMPv6 tests are plotted in Figure 13.6. The lower part shows the itinerary of the vehicle and the locations of AR1 and AR2 on the map, whereas the upper part shows the RTT, the packet loss and the result of the mobility signaling. The X-axis and the Y-axis of the upper part are the latitude and the longitude of the vehicle and correspond to the position of the map in lower part. When either the request or the reply is lost, the RTT is marked as 0, and at the same time, the mark of "packet loss" is drawn. Binding registration success is plotted when the BU and the BA is successfully processed. In contrary, either of them is lost, Binding registration fail is plotted at the position.

[1] https://who.rocq.inria.fr/Manabu.Tsukada/experiments/itsnet/

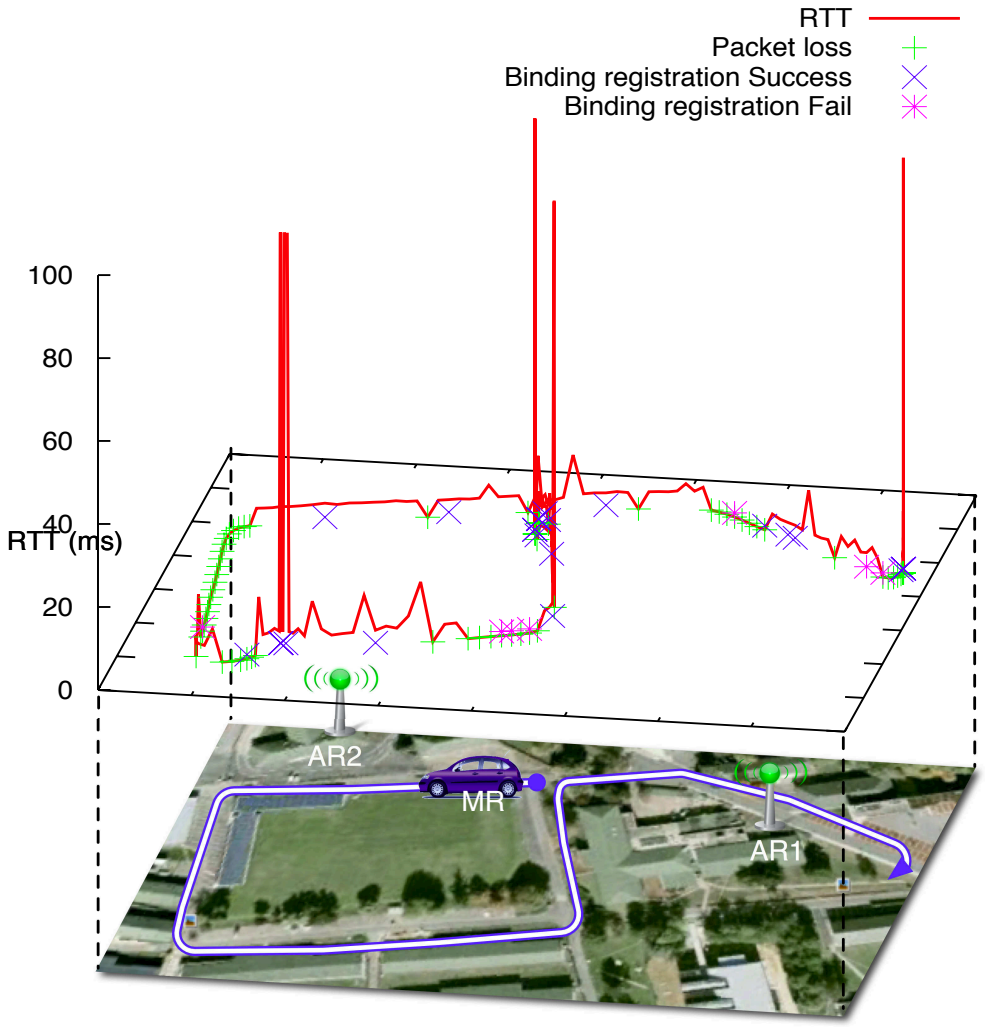


Figure 13.6: RTT, Packet Loss and Mobility Signaling of ICMP evaluation in handover scenario

As can be seen, the RTT is stable with about 5 milliseconds in the beginning of the evaluation. At the period, the MR connects to AR2 that is installed at about 100 meters away, it sent the BU constantly and the binding registration is successfully performed. Soon after the vehicle turns the first corner (north west of the square) the packet starts to be dropped until the second corner. This is because the building shutout the wireless radio. The binding signaling is dropped as well in the period.

The straight road in south of the square is less stable than the one in the north, because of two reasons. First, the location of south straight road is 250 meters farther to AR2 than the one in the north. Thus the signal strength is weaker in the south. Seconds, the trees in meddle of AR2 and the MR interferes the wireless radio. Especially, the trees at the end of the south straight block three consecutive binding messages.

The last straight road in the east has stable wireless radio and no binding message was dropped, while the RTT of two sets of ICMPv6 request and reply exceeds 100 milliseconds. The vehicle approaches to the AR2 along the straight road in the east and turns right to leave from AR2.

The MR starts receiving the RA from AR1 when the distance to AR1 is 50 meters. However the RA from AR2 also reaches to the zone. As the result, the vehicle triggers the movement detection, and sends the mobility signaling via the AR where it receives the RA. When the MR sends the packets to AR2 from the zone, the some ICMP packet and mobility signaling were lost because of the distance and the obstacle (building). When the MR switches to AR1, the packets are stably transmitted.

Figure 13.7 shows the same result of the test with mapping to the time. The upper graph shows the RTT and the distance to the two ARs, the middle shows the PDR to the two ARs, and the lower plots the status of the NEMO signaling. "Success"of NEMO status means the binding registration is successfully performed and "Fail" means either the BU or the BA is lost.

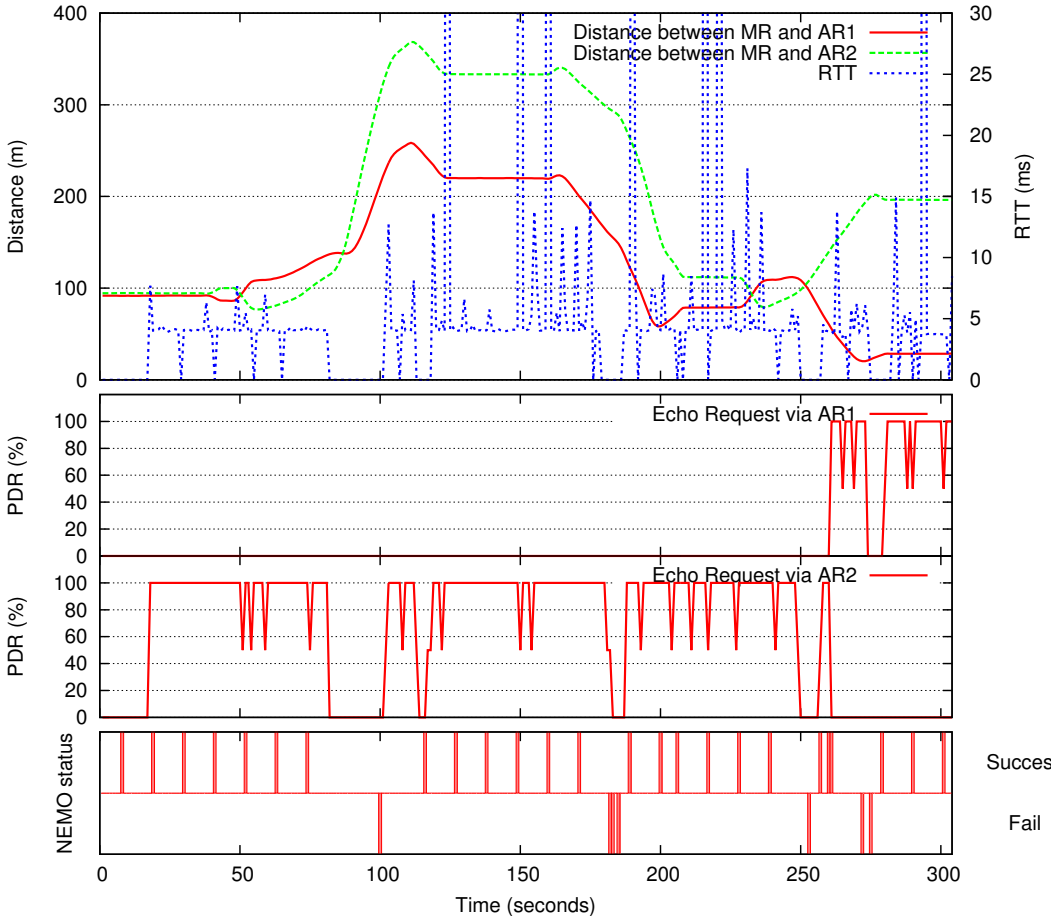


Figure 13.7: RTT, Packet Loss and Mobility Signaling of ICMP evaluation in handover scenario

As can be seen, the RTT and the PDR to AR2 is stable in the north straight road. The binding registrations are done successfully in each 12 seconds interval without packet loss. After the first corner, the packet starts dropping as well as the mobility signaling. Then it recovers when the vehicle comes to the straight road in the south. The mobility signaling is sent again with regular interval.

In the end of the straight road, the ICMPv6 packet is suddenly lost because of the tree in the corner of southeast. At the time, three consecutive binding registrations are lost as

well. When the MR fails to receive a valid matching response within the selected initial retransmission interval, the MR should retransmit the message until a response is received. The retransmission by the MR must use an exponential back-off in which the timeout period is doubled upon each retransmission, until either the MR receives a response or the timeout period reaches the value of maximum timeout period as specified in [rfc6275].

In the case, the MIP6D tried to send the BU one second after the first failure of the binding. Then when it fails, it increases the retransmission time to two, four, eight seconds, and etc. In the case, the BA is returned as a response of forth BU. The disconnection time after the binding registration failure was seven seconds ($= 1 + 2 + 4$).

The east straight road has stable condition for RTT, PDR to AR2 and the NEMO signaling. After turn right to go toward AR1, at the $t = 253$, a mobility signaling is dropped. Then $t = 257$, a binding registration is successfully performed. Actually the registration is transmitted to AR2 because the PDR to AR2 recovers soon after the registration. However $t = 260$ and $t = 261$, the MR receives a RA from AR1 and the trigger the movement. The two BU are successfully registered to the HA and the MR send packets via AR1 (See PDR to AR1 increase at $t = 260$). This time, the handover were possible without any packet loss.

13.2.3 UDP Evaluation in Handover Scenario

In the scenario shown in Section, UDP packets are sent from the MNN to the CN with 1Mbits/sec sending rate with 1250 Bytes packets. The results collected in the ICMPv6 tests are plotted in Figure 13.8. The lower part shows the itinerary of the vehicle and that corresponds to the PDR to the ARs and the binding registration result shown in the upper part, as well as the previous section. As can be seen in the figure, the place is same as the scenario described in the previous section, however the itinerary of the vehicle are reverse direction around the square in this test.

According to the indoor testbed result in Section 13.1.4, the PDR of the UDP configuration is 30%−35%. Actually, the PDR was around 30%−35% in the most stable period in the outdoor testbed in the output of *iperf* as well as the indoor test result. However, the PDR to the two ARs sometimes reaches to 100% as in Figure 13.8. This is because the AnaVANET calculates the PDR based on the MAC address in the air, on the other hand, the bottleneck of the path exist in the CarGeo6 software at that time. In other word, 70% of the UDP packets are dropped in CarGeo6 and the other 30% transmitted from wireless interface were not lost so much. This reason also explains the phenomenon where the binding registration messages are lost while none of the UDP packets are lost (This can be seen in the straight road in the south of the square). In this case, the BUs are lost in the CarGeo6 software and are not transmitted from the wireless interface.

As can be seen, AR2 is only available most of the test period (especially, around the square) except for the end of the test. When the vehicle runs in the first straight road in the east, the PDR to AR2 is almost 100%. During this period, no binding message was dropped. The BUs are sent regularly with 12 seconds interval.

In contrary, all the binding registrations are lost in the south straight road. After the first packet loss of mobility signaling, the binding registration continuously fails until the vehicle goes around and arrives at the area of AR1. Thus the UDP packet does not arrives at CN during the period, because the HA does not has the binding and discard the tunneled packet from the MR. The MR sends tunneled UDP packets to the HA during the period where the mobility signaling fails. The PDR to AR2 shows over 80% of the packets from the MR are delivered to the AR2 constantly, when the vehicle runs in the south straight road.

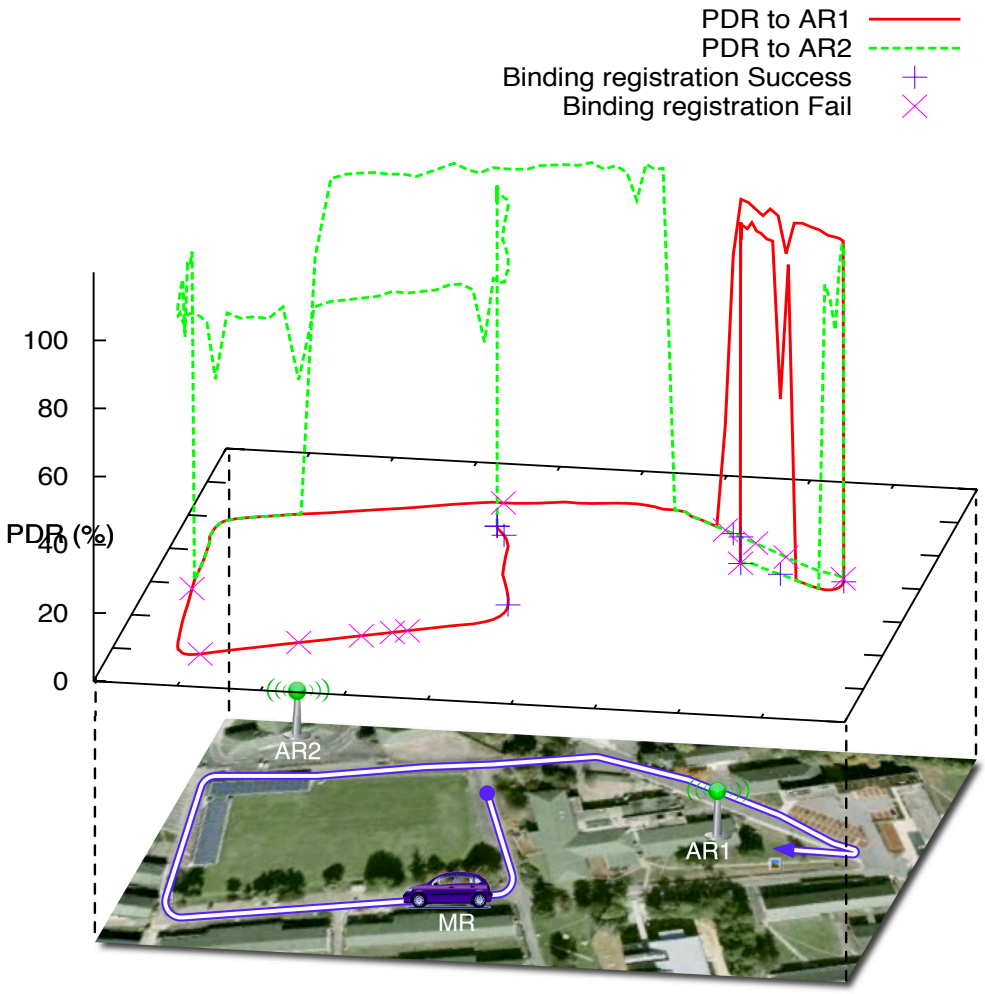


Figure 13.8: PDR to the two ARs and Mobility Signaling of UDP evaluation in handover scenario

The packets start being dropped on the west of the square because the building on the north west corner of the square blocks the wireless radio. When the beacons exchanged between GeoNetworking nodes twice in a second are dropped, the correspondent entry of the location table expires in 5 seconds, because the lifetime of the location table entries are configured as 5 seconds.

When the vehicle approaches at 20 meters from AR1, a binding registration with the CoA obtained in AR's access network is successfully performed. The path to the Internet is switched via AR1 at the moment. The PDR to the AR1 shows almost 100% packets are delivered from the MR to the AR1. The RA from AR2 sometimes reaches to the area, and the MR makes a binding registration with the CoA obtained from AR2. The path to the Internet is switched via AR2 again. Since the MR receives the RAs from both AR1 and AR2 at the area, the MR detects the movement when it receives the new different RA from the previous one.

Figure 13.9 shows the same test with mapping to the time. The upper graph shows the Throughput of UDP from the MNN to the CN, the middle part shows the PDR to the two ARs, and the lower plots the status of the NEMO signaling. Success"of NEMO status means

the binding registration is successfully performed and "Fail" means either the BU or the BA is lost.

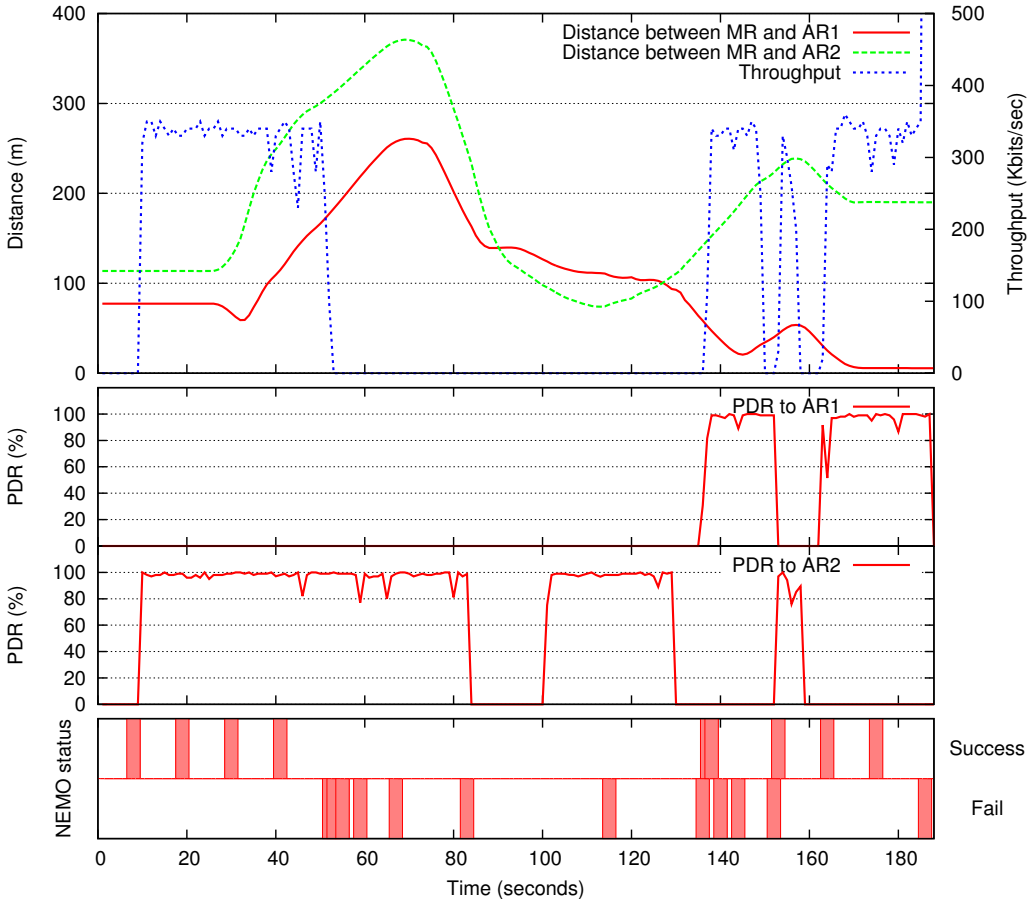


Figure 13.9: PDR to the two AR and Mobility Signaling of UDP evaluation in handover scenario

As can be seen, the throughput from the MNN to the CN, and the PDR to AR2 is stable in the beginning of the test (the vehicle is 80 meters away from AR2 in the north east of the square). The binding registrations are done successfully in each 12 seconds interval without packet loss. After the first corner, the throughput drops to zero as well as the binding registration fails, while the PDR to AR2 is still almost 100%. This shows the mobility signaling packets are lost in CarGeo6 as mention in the beginning of this section. Since the binding fails, the HA dos not have the binding for the MR and discard the packet from the MR. The interval of the BUs are increased exponentially from 1 seconds to 32 seconds (1, 2, 4, 8, 16 and 32 seconds).

Then at $t = 139$, when the vehicle is 20 meters away from AR1, the first binding registration of the CoA from AR1 success. The UDP packets are switched to AR1 from the moment. Then at $t = 155$, the binding registration is successfully performed via AR2 again. During the handover from AR1 to AR2 from $t = 155$ to $t = 158$, three seconds of disconnection are counted in the *iperf* log. At $t = 166$, the path to the Internet is switched to AR1 again. At this handover, the UDP packets are lost during 4 seconds from $t = 166$.

13.3 Conclusion

Indoor tests show the network performance using CarGeo6 in terms of delay and throughput. In single hop test, the delay was about 5 ms, that is as small as the one using GeoNet implementations. However, the delay on multi-hop has about 35 ms, which is twice bigger than the one using the GeoNet one. The maximum UDP throughput using CarGeo6 in single hops is around 400 Kbits/sec, that is ten times smaller than the one using GeoNet one. The bigger delay and smaller throughput using CarGeo6 are explained by two reasons. The two non-standard optimization works implemented in the GeoNet implementations (the next hop IPv6 address cache and multi-hop beaconing) is not implemented in CarGeo6. Thus the CarGeo6 resolves the next hop IPv6 address from the routing table for each forwarding packet regardless of either single hop or multi-hop. This increase the processing delay in the source MR. In addition, in multi-hop case, the source MR launches the location service in request-reply manner for all the forwarding packet. This causes the additional processing delay and signaling delay.

The outdoor test using NEMO left as a future work in the GeoNet project is performed using CarGeo6. ICMPv6 and UDP evaluations in handover scenarios were performed in INRIA Paris-Rocquencourt campus with two ARs. In all the tests, the line of sight between the vehicle and the roadside ITS Station has been a key factor to maintain communication links. The communication between them are disturbed by the trees not only the buildings. When the signaling packet (*i.e.* Binding Update (BU) and Binding Acknowledgement (BA)) is dropped, the disconnection last long time. From the test, we confirm the packets are dropped in the CarGeo6 GeoNetworking modules and they are not dropped in the air.

Part IV

Conclusions and Future work

Conclusions

In this dissertation, we have studied how the communication can be optimized between vehicle and its communication peers by selecting the appropriate communication path using all possible types of information in Cooperative ITS. First, we presented all the pieces on which our work is based: the Cooperative ITS activities; the terminology; the ITS Station reference architecture; the access layer technologies; the network layer protocols, particularly IPv6 and the mobility protocols (Part I). In Chapter 4, we highlighted issues and design requirements to realize intelligent path selection and IPv6 GeoNetworking within the ITS Station architecture. We concluded that path selection need to manage three types of paths between vehicles: *Anchored path*, *optimized path* and *direct path*. We proposed a cross-layer improved path selection decision-making algorithm using information from various layers of the ITS Station reference architecture stack in cooperative ITS. The study resulted in the three major propositions: Path selection manager (Chapter 6), Cross-layer path selection parameters and primitives (Chapter 7) and IPv6 GeoNetworking (Chapter 8).

In order to fit these propositions into the ISO/ETSI ITS Station architecture, we presented our approach to abstract the parameters exchanged between the management entity and the network layer (Chapter 5). Following this approach, we could design more comprehensive definition of exchanged parameters than the way to just list up the parameters to fit the needs, that can be found in the current ISO specifications. In this dissertations, we focused on the parameters related to path selection, however we believe the approach can be applied to the other topics (*e.g.* Quality of Service, Multicast, etc.). We also believe the presented approach can be a reference for designing the exchange of parameters between the other layers and the management entity (*i.e.* MF-SAP and MI-SAP). This is because our abstraction approach makes the cross-layer functions independent from any specific protocol.

In Chapter 6, we have proposed three categories of information used by the path selection manager maintained in the management entity: *ITS Station information table*, *path information table* and *flow requirement table*. The parameters are defined as needed by the path selection manager, however the parameters can be used for the other cross-layer function (*e.g.* Service Discovery), because the parameters are abstracted with the notion of nodes (or vertices) and links (or edges) which is valid for any kind of networking. The path selection manager is designed as a replaceable module in the ITS Station stack. This allows progressive improvement of the decision-making process. In this dissertation, we have presented a geographic information based path calculation and an application of Multiple Attribute Decision Making (MADM) method to the path selection decision-making algorithm.

In addition to the primitives specified in ISO standards (*MN-REQUEST* and *MN-COMMAND*), we have defined new primitives (*MN-GET* and *MN-SET*) in order to reuse the Management Information Base (MIB) specifications of the network layer protocol blocks (Chapter 7). By introducing the newly defined primitives, we could avoid maintaining a duplicate MIB in the management entity. Following the ISO specification of *MN-SAP*, we have defined five new *MN-REQUEST* commands and three *MN-COMMAND* commands in order to enable cross-layer path selection. This is not limited to the path selection in the IP-based nor GeoNetworking-based network thanks to the abstraction of the parameters at the management entity level, even though our study has focused on IPv6 GeoNetworking.

The basic IPv6 GeoNetworking specification has been made under the framework of the GeoNet project (Chapter 8). Our contributions for the project was developing the interface between IPv6 and GeoNetworking (Geo-IP SAP), and results finally have been published in the GeoNet project deliverable [GeoNet-D.2]. Earlier in the project, we (IN-

RIA) have made a set of propositions for combining IPv6 and GeoNetworking available in [Tsukada2009]. Thanks to the standardization effort by some of the GeoNet project members after the project completion, some results of this work can be seen in ETSI standards [ETSI-TS-102-636-3-GeoNetworking-Arch, ETSI-TS-102-636-6-1-IPv6-GeoNetworking], today. As the GeoNet project was a challenging project, it has concentrated on the core functions of IPv6 GeoNetworking. For this reason, the GeoNetworking link was initially defined as simple as possible to make the core discussion easier. After the project, thus we have proposed the end based geographic link model in order to alleviate the constraints that an IPv6 subnet is restricted to a geographic area.

The source codes of Geo-IP SAP that we have implemented in the GeoNet project was integrated with the GeoNetworking implementations by HITACHI and NEC [GeoNet-D.3, GeoNet-D.6]. Later, the source code was also integrated with a new implementation of GeoNetworking (CarGeo6) (Chapter 9) and publicly available as an open source distribution. On the other hand, the implementation of simultaneous usage of multiple paths was made under the ANEMONE project [Montavont2008a]. The IPv6 testbed constructed in ANEMONE project was used for the evaluation of the implementation.

The evaluations using these implementations have been performed on either the ANEMONE testbed or the LaRA testbed. We have developed the AnaVANET tool in order to analyze the impact of various conditions to the metrics for outdoor test evaluation. Indoor evaluation result shows the IPv6 GeoNetworking implementation can offer sufficient performance of communication in terms of average delay and maximum throughput (5 ms and 4500Kbps on single hop / 15ms and 1350Kbps on multi-hop, respectively). However the results also show that the bigger delay and smaller throughput using CarGeo6 which does not have the two proposed optimization works (*next hop IPv6 address cache* and *multi-hop beaconing*). The outdoor evaluation result shows, in all the tests, the line of sight between vehicles has been a key factor to maintain communication links. Moreover, the number of hops used in transmission paths, has been identified as another key performance. We also proofed that the network performance can be increased by combining the anchored path (NEMO path) and the direct path (MANET path).

The evaluation result of simultaneous usage of anchored path and direct path using the ANEMONE testbed or the LaRA testbed are published in [Tsukada2008, Tsukada2010a]. As a benchmark, the network performance of a VANET maintained by a standard MANET protocol (OLSR) has been measured using AnaVANET. This work has been published in [Santa2009b, Santa2009a]. The GeoNet implementations have been evaluated in LaRA indoor and outdoor testbeds using AnaVANET and the results have been reported in the GeoNet project deliverable [GeoNet-D.7] and also in conference papers [Tsukada2010b, Ines2010]. The application and the network configuration used in the final demonstration of the GeoNet project also has been published in [Noguchi2011]. The evaluation of CarGeo6 has been published in [Toukabri2011].

Future work

Our study has only focused on the cross-layer path selection in a single ITS Station router. The single ITS Station collects the network information as much as possible to make an intelligent path selection decision, however in reality, a single router can not manage the entire paths. Assuming that vehicle ITS Stations (A and B) communicate via the Internet (*i.e.* Roadside-based or Internet-based communication mode). The controllable path by vehicle ITS Station A could be typically the portion of the anchored path from the ITS

Station to the anchor which supports mobility of the ITS Station. If ITS Station A needs to the control further portion of the path beyond the anchor, ITS Station A needs to *collaborate* with ITS Station B. Moreover, an ITS Station router must collaborate to other ITS Station to control the portion of the path that cannot be directly controlled by itself. Thus in the future, we would like to investigate how the collaboration between ITS Stations can be performed to control larger portions of the path than the standalone path selection presented in this dissertation. We consider an approach for the collaboration could be the exchange of the management parameters defined in the dissertation between the ITS Stations, however we need more investigation to enable the inter-ITS Station collaboration for path selection.

Our solutions for path selection relies on the assumption that the application requirements are simply provided from the facilities layer to the management entity. However in reality, the acquisition of the application requirements can be more complicated, because the application and the routing function are divided into more then one node following the router and host split concept in the ITS Station architecture presented in Section 4.2.3. To make the ITS Station host application requirements available in the ITS Station router, the application requirements must be exchanged between the hosts and router. We consider there are two possible approaches. First, the application requirements are exchanged as a facilities layer function between the host and the router. Second solution can be the ITS Station internal management entity collaboration between the hosts and the router. There is a similarity of the second solution and the inter-ITS Station management entity collaboration described above besides that the management parameters are transferred between the nodes composing the ITS Station in one case, and between ITS Station in the other case.

The path selection manager algorithm itself has rooms to be improved. For example, we introduced a geographic position and movement based path calculation to predict the path status. The path calculation could be able to be more precise with additional information, for example, map information, car destination, road traffic information, etc. In this dissertation, we have applied MADM method to the path selection decision-making algorithm. The *weights* of each parameters used in MADM method should be determined to fit the communication scenarios in cooperative ITS in the future. On the other hand, since the method can be replaced thanks to the path selection manager design, thus we are also interested in replacing it by a better algorithm. In addition to the adjustment of the weights and improvement of the algorithm, we must also keep considering new parameters obtained from the other layers (*e.g.* the facilities layer). Local Dynamic Map (LDM) currently being developed function to meet cooperative ITS requirements must be able to provide valuable information for the path selection manger.

The path selection problem can be seen as a network resource allocation problem (*e.g.* bandwidth). From a resource allocation point of view, the path selection is not always the best solution. For example, when the network resource is limited, reducing the network traffic from the applications is more efficient than the best intelligent path selection. Thus there is a need for the adaptive application in the environment where the network conditions change dynamically. To make the application in the hosts adaptive to the network condition, the network condition must be shared internally in the ITS Station. As well as the ITS Station internal network condition sharing, the inter-ITS Station network status condition is needed to change application behavior of the hosts within the ITS Station. As the network condition is stored in the management tables defined in the dissertation, the exchange of the parameters could be a solution for adaptive application. We need to investigate this more.

A ITS Station router is aware that which flow goes through which path as a result of path selection as well as the characteristic of each path. A host runs application can change the

transport layer protocol applied to the flows depending on the path for the flows using the information available in the ITS Station router. For example, the mobility-aware transport layer protocol should be applied for flow goes through the path frequently change the point of attachment in access network.

We have proposed the geographic information management based on ITS Stations information table. As examples, we have shown that ITS Station acquires the neighbor ITS Station's geographic information by either GeoNetworking beaconing in the network layer or the CAM in the facilities layer. However in both protocols the acquisition of the geographic information of the neighbor ITS Station is limited to the area where the broadcast messages are distributed. We need a means to exchange the geographic information between ITS Stations remotely located. For example, the geographic position of the anchors can be considered as an important metric to select the anchor used for mobility support.

The evaluation shows network performance using CarGeo6 implementation should be improved, especially in multi-hop communication. We saw as an experiment result, the *next hop IPv6 address cache* and *multi-hop beaconing* implemented in the two implementations in the GeoNet project can be the candidates of the improvement. We need to investigate that how much cache is effective in which case, how many multi-hop is effective in which case.

Part V

Appendix

Appendix A

Sixth Framework Programme (FP6)

Figure A.1: The logo of Sixth Framework Programme (FP6)

Sixth Framework Programme (FP6) is the European research and development plan for 4 years from 2002 to 2006. The total founding was 17.5 billion euros (average 4.4 billion euros in a year). The ITS related projects are listed in the following table. Each row shows project logo, number of partners, number of countries, period, budget in euros and the abstract. This information is published in Community Research and Development Information Service (CORDIS) [1] and one can search by putting the name of the project in the search window. In Sixth Framework Programme, there are forty five ITS related projects and 381.7 millions of euros are spent for the projects. The biggest projects are Prevent which spent 54 million euros, CVIS for 41 million euros, Safespot for 38 million euros, and Coopers for 16.8 million euros.

Project	Partners	Period	Budget	Keywords
ATESST	10 partners, 4 countries	Jan 2006 - Mar 2008	€ 3.9 M	The basis of the **ATESST** project is the architecture description language EAST-ADL2, developed in the ATESST project. The language provides an information structure and ontology that makes the development of stand-alone automotive embedded systems more systematic and predictable.
aide	28 Partners	Mar 2004 - Feb 2008	€ 12.6 M	The general objective of the **AIDE** (Adaptive Integrated Driver-Vehicle Interface) is to generate the knowledge and develop methodologies and human-machine interface technologies required for safe and efficient integration of Advanced Driver Assistance Systems (ADAS) and In-vehicle Information Systems (IVIS) and nomad devices into the driving environment.

[1] http://cordis.europa.eu/

Project	Partners	Period	Budget	Keywords
AIRNET	5 partners, 3 countries	Jan 2004 - Dec 2006	€ 2.6 M	**AIRNET** aims at developing and testing an EGNOS low-cost platform for the surveillance, control and management of airport vehicles.
C2R	12 partners, 5 countries	Jan 2006 - Dec 2007	€ 5.6 M	**COM2REACT**'s overall objective is to establish the feasibility of such a three-layer, scalable, cooperative system.
COMeSafety	6 partners, 3 countries	Feb 2006 - Dec 2009	€ 1.5 M	**COMeSafety** provides an open integrating platform for both the exchange of information and the presentation of results, aiming for the interests of all public and private stakeholders to be represented.
coopers	37 partners, 14 countries	Feb 2006 - Feb 2010	€ 16.8 M	The Mission of **COOPERS** (Co-operative Networks for intelligent Road Safety): to define, develop and test new safety related services and equipment and applications using two- way-communication between road infrastructure and vehicles from a traffic management perspective.
Cover	9 partners, 4 countries	Mar 2006 - Feb 2009	€ 4.1 M	**COVER** (Semantic-driven cooperative vehicle infrastructure systems for advanced e-safety applications) will foster the creation of the next generation intelligent cooperative systems that will make road transport more efficient and effective, safer and more environmentally friendly.
CVIS	61 partners, 12 countries	Feb 2006 - Feb. 2010	€ 41.0 M	**CVIS** (Cooperative Vehicle-Infrastructure Systems) aims to design, develop and test new technologies needed to allow vehicles to communicate with each other and with the nearby roadside infrastructure.
CyberCars²	12 partners, 6 countries	Jan 2006 - Dec 2008	€ 4.0 M	**CyberCars-2** extends and complements the valuable work done by CyberCars and CyberMove projects of the 5th Framework Program by addressing high demand and more cooperation between vehicles.
EASIS	22 partners	Jan 2004 - Mar 2007	9.6 M	**EASIS** (Electronic Architecture and System Engineering for Integrated Safety Systems) contributes to increased road safety by developing a standardised, highly dependable in-vehicle electronic architecture for active, passive and integrated safety systems.
FeedMAP	14 partners, 7 countries	Mar 2006 - Aug 2008	€ 3.6 M	**FeedMAP** (Technical and commercial feasibility assessment of map data feedback loops applied to the ActMAP framework) project develops a framework that will allow for easier and faster updating of digital maps.
ANEMONE	7 partners, 4 countries	Dec 2006 - Aug 2008	€ 3.3 M	The primary goal of the **ANEMONE** project is to provide them with such a playground and help inventing tomorrow's world.

Project	Partners	Period	Budget	Keywords
FRICTI@N	10 partners, 5 countries	Jan 2006 - Dec 2008	€ 4.3 M	The **FRICTI@N** project improves road safety by providing vehicles with the information needed in longitudinal & lateral control and in emergency braking systems.
GOOD ROUTE	12 partners, 6 coutries	Jan 2006 - Dec 2008	€ 4.9 M	**GOOD ROUTE** (Dangerous Goods Transportation Routing, Monitoring and Enforcement) aims to make European road transportation safer by providing Dangerous Goods Vehicles (DGV) with a validated and integrated Dangerous Goods Transportation Routing, Monitoring and Enforcement cooperative system.
GST	55 partners	Mar 2004 - Mar 2007	€ 22.1 M	**GST** will create an open and standardized framework architecture for end-to-end telematics.
Highway	9 partners, 3 countries	Apr 2004 - Dec 2006	€ 4.8 M	**HIGHWAY** offers higher safety and location-based value added services where interactions between the person in control, the vehicle and the information infrastructure are addressed in an integrated way.
humanist	23 partners	Mar 2004 - Feb. 2008	€ 5.3 M	**HUMANIST** is a Network of Excellence (NoE). Its goal is to create a European Virtual Centre of Excellence on HUMAN centred design for Information Society Technologies applied to Road Transport.
Im@gine It	16 partners, 5 countries	Jan 2004 - Dec 2005	€ 4.5 M	**IM@GINE IT** supports the eSafety initiative by performing research in distributed intelligent agents, secure communications and advanced positioning and mapping technologies and their integration, to offer safe, personalised, location-based value- added services.
ISHTAR	6 partners, 5 countries	May 2005 - Dec 2006	€ 0.7 M	The main objective of the **ISHTAR** SSA project is to contribute towards the harmonisation of technologies, services/applications, and standardisation efforts in the field of Location Based Services (LBS).
ISMAEL	8 partners, 4 countries	Feb 2004 - Jan 2007	€ 3.6 M	**ISMAEL** aims to determine whether recent advances in magnetic sensors could provide a better means of surface movement surveillance at airports.
i-way	13 partners, 8 countries	Feb 2006 - Jan 2009	€ 4.6 M	**I-WAY** aims to enhance drivers perception on road environment and improve his responses in time critical traffic scenarios by providing real time information from other vehicles in the vicinity and from effectively located roadside equipment as well.

Project	Partners	Period	Budget	Keywords
	10 partners, 5 countries	Jan 2006 - Mar 2008	€ 4.1 M	**MORYNE** provides an effective cooperative system, by using public transport vehicles as elements of a network of mobile sensors, communicating with the infrastructure, and setting up co-operation between public traffic management and city traffic management.
	60 pertners, 15 coutries	Feb 2004 - Mar 2008	€ 54.1 M	**PReVENT**(Preventive and Active Safety Applications) develops, tests and evaluates safety related applications, using advanced sensor and communication devices integrated into on-board systems for driver assistance.
	4 pertners, 3 coutries	Jan 2006 - Dec 2007	€ 1 M	**REPOSIT** (RElative POSitioning for collIsion avoidance sysTem) develops a novel concept to prevent accidents through collision avoidance based on Vehicle to Vehicle (V2V) communication.
	51 partners, 12 countries	Feb 2006 - Feb. 2010	€ 38.0 M	The basic concept of **SAFESPOT** is to use both vehicles and infrastructure as sources and destination of safety-related information.
	7 Partners, 5 countries	Jan 2006 - Dec 2008	€ 4.5 M	**SeVeCom** focuses on providing a full definition and implementation of security requirements for vehicular communications.
	10 partners,	Jan 2005 - Dec 2007	€ 3.6 M	**REACT** will develop a system that will work towards the Community's objectives of reducing road transport deaths and increasing road infrastructure capacity.
	13 partners, 6 countries	Jan 2004 - Dec 2006	€ 2.6 M	**eIMPACT** assesses the socio-economic effects of Intelligent Vehicle Safety Systems (IVSS), their impact on traffic safety and efficiency.
	4 partners, 3 countries	Jan 2006 - Dec 2008	€ 2.3 M	**eSafety Support** monitors the progress on each of the 28 eSafety priority recommendations through close cooperation with the eSafety Forum Working Groups.
	1 partner, 1 counties	Dec 2003 - Dec 2005	€ 0.6 M	**eSCOPE** is an eSafety Observatory established to monitor the activities of the eSafety initiative and to stimulate their progress.
	2 partners, 2 countries	Dec 2005 - May 2007	€ 0.3 M	**EU-India** aims to improve road safety and the efficiency of transportation systems in India through a close cooperation between European and Indian stakeholders defining key issues for ITS deployment and in particular Intelligent Integrated Safety Systems (eSafety) in India.
	17 partners, 6 countries	Mar 2004 - May 2007	€ 3.1 M	**EURAMP** focuses on ramp metering control measures on European motorways aiming at improving safety and increasing efficiency of the traffic flow.

Project	Partners	Period	Budget	Keywords
	14 partners	Sep 2004 - Oct 2006	€ 2.8 M	**MITRA** aims to develop a prototype central information system for high-risk and dangerous roads being transported across Europe by road or rail.
	6 partners, 3 countries	Jan 2004 - Jun 2005	€ 1.8 M	The **SAFE-AIRPORT** project involves the development of an innovative acoustic system based on two Passive Phased Array Microphone Antennas capable of detecting and tracking aeroplanes within a range of at least six nautical miles in the air and on the ground.
	6 partners, 3 countries	Jan 2004 - Jun 2006	€ 1.8 M	**SAFETEL** aims at improving the design standards of equipment and systems in the automotive world providing advanced tools for prediction, design and testing, in order to enhance the susceptibility hardening of motor vehicles against electromagnetic (EM) disturbances.
	5 partners, 2 countries	Oct 2006 - Sep 2008	€ 0.6 M	**SAFETY-TECHNOPRO** is a Training System on New Safety Technologies for Road Transport Addressed to Professional Bodies of the Automotive Sector.
	2 partners, 2 countries			**SEiSS** analyses the socio-economic effects of intelligent safety systems in road vehicles. Road crashes take a tremendous human and societal toll from all member states.
	20 partners, 8 countries	Jan 2004 - Dec 2006	€ 13.3 M	**SPARC** contributes to overall road safety and traffic efficiency by integrating x-by-wire technologies into the powertrain for both heavy goods vehicles and passenger cars.
	18 partners 10 countries	Nov 2006 - Oct 2009	€ 10.5 M	**SISTER** (Satcoms in Support of Transport on European Roads) aims to promote the integration of satellite and terrestrial communications with GALILEO to enable mass market take-up by road transport applications.
	16 partners - 8 countries	Jan 2006 - Jun 2008	€ 4.0 M	**TRACE** focuses on accident causation analysis and the evaluation of safety benefits of technologies.
	14 partners, 13 countries	Jan 2006 - Oct 2008	€ 4.4 M	**TRACKSS** tackles this challenge by working on both in-vehicle sensors and infrastructure sensing technologies.
	13 partners, 6 countries	Jan 2006 - Oct 2008	€ 5.9 M	**WATCH-OVER** designs and develops a cooperative system for the prevention of road accidents involving vulnerable road users in urban and extra-urban scenarios.

Project	Partners	Period	Budget	Keywords
FIDEUS Freight Intelligent Delivery of Goods in European Urban Spaces	14 partners	May 2006 - Dec 2008	€ 4.4 M	The **FIDEUS** project is to provide a complementary set of vehicle solutions to support an innovative approach to the organisation of urban freight transport, in line with political strategies to safeguard the "liveability" of cities, while being compatible with efficient logistics.
	46 partners	Nov 2003 - Apr 2006	€ 25.7 M	The objective of **Daidalos** is to develop and demonstrate an open architecture based on a common network protocol (IPv6), that becomes a significant step towards approaching the Daidalos vision.
	37 partners	Jan 2006 - Dec 2008	€ 22.1 M	**Daidalos phase 2** continues the works from Daidalos phase 1 and improves them.
HEAVY ROUTE	7 partners	Sep 2006 - Jun 2009	€ 3.3 M	The **HeavyRoute** project aims to develop an advanced route guidance system for HGVs as a tool for deriving the safest and the most cost effective routes for road freight transports throughout Europe.
intro	10 partners, 7 countries	Mar 2005 - Feb 2008	€ 3.5 M	**INTRO** develops innovative methods for increased capacity and safety of the road network.

Appendix B

Seventh Framework Programme (FP7)

Seventh Framework Programme (FP7) is the European research and development plan for 7 years from 2007 to 2013. The total founding will be 50.5 billion euros (average 7 billion euros in a year). The ITS related projects are listed in the following table. Each row shows project logo, number of partners, number of countries, period, budget in euros and the abstract. This information is published in Community Research and Development Information Service (CORDIS)[1] and one can search by putting the name of the project in the search window.

In Seventh Framework Programme, there are 29 ITS related projects and 184.2 millions of euros are spent for the projects. Note that the table is updated at June 2010 and FP7 will surely continue working on ITS related project. The biggest project is HAVE-IT (28 million euros), teleFOT (14 million euros) and euroFOT (14 million euros).

Figure B.1: The logo of Seventh Framework Programme (FP7)

Project	Partners	Period	Budget	Keywords
2wide sense	7 partners, 4 countries	Jan 2010 - Dec 2012	€ 5.1 M	The **2WIDE_SENSE** project aims at providing European automotive industry with the next generation of imaging sensors beyond the current CMOS imagers.
ADOSE	11 partners, 8 countries	Jan 2008 - Dec 2010	€ 10.2 M	**ADOSE** addresses research challenges in the area of accident prevention through improved-sensing technologies and sensor fusion.
ARTIC	10 partners, 9 countries	2008 - Feb 2010	€ 0.5 M	The **ARTIC** project aims at spreading the latest antenna technologies towards the automotive application area.
ATESST	10 partners, 4 countries	Jul 2008 - Jul 2010	€ 3.8 M	During **ATESST2**, the EAST ADL2 will be refined to better support automotive systems development, in particular cooperative active safety systems.

[1] http://cordis.europa.eu/

Project	Partners	Period	Budget	Keywords
eCoMove	32 partners, 10 countries	Apr 2010 - Mar 2013	€ 22.7 M	The **eCoMove** project creates an integrated solution for road transport energy efficiency by developing systems and tools to help drivers sustainably eliminate unnecessary fuel consumption, and to help road operators manage traffic in the most energy-efficient way.
FRAME	7 partners	May 2008 - May 2011	€ 1.6 M	**E-FRAME** provides support for the creation of interoperable and scalable Cooperative Systems throughout the European Union. It will provide a centre of knowledge that is commercially and politically neutral, and which services everyone's long term interests.
Safety Aware	6 partners, 4 countries	Jan 2010 - Dec 2011	€ 1.8 M	**eSafetyAware!** seeks to accelerate the market introduction of life-saving technologies by organising information campaigns and dedicated events aimed at creating awareness of eSafety benefits among policy-makers and end-users.
URIDICE	22 partners, 9 countries	Jan 2008 - Dec 2010	€ 14 M	The basic concept of **Euridice** is to build an information services platform centred on the individual cargo item and on its interaction with the surrounding environment and the user.
euroFOT	28 partners	May 2008 - Aug 2011	€ 13.9 M	The goal of **EuroFOT** is to identify and coordinate an in-the-field testing of new Intelligent Vehicle Systems with the potential for improving the quality of European road traffic.
eVALUE	8 partners, 4 countries	Jan 2008 - Dec 2010	€ 3.7 M	The main focus of project **eVALUE** (Testing and Evaluation Methods for ICT- based Safety Systems) is to define objective methods for the assessment of ICT- based, preventive road safety systems.
evita	12 partners, 5 countries	Jul 2008 - Jun 2011	€ 6 M	**EVITA** designs, verifies, and prototypes an architecture for automotive on-board networks where security-relevant components are protected against tampering and sensitive data are protected against compromise.
IFM FORUM	8 partners, 4 countries	Jan 2008 - Dec 2009	€ 0.9 M	**IFM**-project aims to make public transport more user-friendly through facilitating network access.
FESTA	22 partners, 8 countries	Nov 2007 - Jun 2008	€ 2.1 M	The **FESTA** Support Action is a vital step in the realisation of scientifically robust and efficiently run Field Operational Tests which aim to evaluate key ICT functions.
FNIR	6 partners, 4 countris	Jan 2008 - Jun 2010	€ 3.1 M	The **FNIR** project is to demonstrate the next generation Night Vision System with automatic detection of upcoming hazards at an affordable cost.

Project	Partners	Period	Budget	Keywords
FOT-NET	9 partners, 7 countries	Jun 2008 - Aug 2010	€ 1.2 M	**FOT-Net** aims at supporting the European Commission in bringing together European and international stakeholders to form a strategic networking platform.
GeoNet	7 partners, 6 countries	Feb 2008 - Feb 2010	€ 3.0 M	**GeoNet** is thus committed to address this gap by combining geonetworking and IPv6 into a single communication architecture, that is referred as IPv6 geonetworking. The combination of geonetworking and IPv6 will allow for both IPv6 and non-IPv6 communications.
HAVEit	18 partners, 8 countries	Feb 2008 - Jul 2011	€ 27.8 M	**HAVE-IT** will develop 6 next generation highly automated ADAS systems aiming at improved comfort, safety and efficiency.
INTERSAFE2	10 partners - 7 countries	Jun 2008 - May 2011	€ 6.5 M	The general objectives of **INTERSAFE-2** are to develop and demonstrate a Cooperative Intersection Safety System (CISS) capable of significantly improving traffic safety at intersections.
iTETRIS	9 partners, 5 contries	Jul 2008 - Dec 2010	€ 4.5 M	**iTETRIS**' vision is to create a global, sustainable and open vehicular communication and traffic simulation platform.
Nearctis	8 partners, 6 countries	Jul 2008 - Jun 2012	€ 3.1 M	The **NEARCTIS** project aims at bringing together most of the European academic community working on road traffic management, traffic control, communications and location technologies.
oversee	8 partners, 4 countries	Jan 2010 - Jun 2012	€ 3.9 M	**OVERSEE** realizes an open vehicular IT platform that provides a protected standardized in-vehicle runtime environment and onboard access and communication point.
PRECIOSA	4 partners, 2 countries	Mar 2008 - Feb 2010	€ 2.5 M	The goal of **PRECIOSA** is to demonstrate that co-operative systems can comply with future privacy regulations by demonstrating that an example application can be endowed with technologies for suitable privacy protection of location related data.
PRE-DRIVE C2X	23 partners, 9 countries	Jul 2008 - Jul 2010	€ 8.5 M	**PRE-DRIVE C2X** develops a detailed system specification and a functionally verified prototype robust enough to be used in future field operational tests.
ROADIDEA	14 partners, 9 countries	Dec 2007 - May 2010	€ 4.9 M	**ROADIDEA** looks for new ideas to combine traffic and weather data into new services using brainstorm and idea generation techniques.
ROSATTE	18 partners, 11 countries	Jan 2008 - Jun 2010	€ 4.7 M	The **ROSATTE** project aims at establishing an efficient and quality ensured data supply chain from public authorities to commercial map providers with regards to safety related content.

Project	Partners	Period	Budget	Keywords
	19 partners, 7 countries	Jan 2008 - Jun 2010	€ 5.4 M	**SAFERIDER** aims to study the potential of ADAS/IVIS integration on motorcycles for the most crucial functionalities and develop efficient and rider-friendly interfaces and interaction elements for riders comfort and safety.
	2 partners, 2 countries	Jan 2008 - Jun 2010	€ 1.4 M	**Thinkingcars** produces a high quality television video documentary to raise public awareness of eSafety systems via mass media broadcasting.
	10 partners, 7 countries	Jan 2008 - Jun 2010	€ 3.0 M	The **SMARTFREIGHT** project wants to make urban freight transport more effi- cient, environmentally friendly and safe through the smarter use of distribu- tion networks and better delivery and return freight systems.
	24 partners, 10 countries	Jun 2008 - May 2012	€ 14.4 M	**TeleFOT** assesses the impacts of functions provided by aftermarket and nomadic devices in vehicles by large scale field operational tests and raises wide awareness of these impacts.

Appendix C

Existing Specification of Management in ISO

Appendix C shows the management parameters that are currently specified in the ISO standard [ISO-24102-1-ITSS-management, ISO-24102-2-Management-SAP]. Note that this study is based on year 2011 versions of the ISO Standards and that the standards constantly evolve. As a result, the ISO specifications in Appendix C may have changed at the time of reading.

Table C.1 shows the existing management parameters specified in [ISO-24102-1-ITSS-management]. Concerning to path selection, some parameters have relation with interface selection:

- *MinPrioCrossCI*
- *VciList*
- *CrossCiPrioList*
- *VCIperformList*

The other parameters are also related to path selection such as geographical information of self ITS Station and application requirements:

- *StationPosition*
- *ITSSI*
- *ApplReqList*

Table C.2 shows the parameters of ITS State Information (ITSSI) specified in [ISO-24102-1-ITSS-management]. This management parameter only stores the the mapping of Station ID, Station type and the position of the station and thus cannot fulfill the design requirements of the study presented in Chapter 4.

Parameter name	Description
StationID	Identifier of ITS station. Preferably globally unique.
MinPrioCrossCI	Minimum user priority required for cross-CI prioritization.
StationPosition	Actual kinematics vector of station. Timestamp, latitude, longitude, altitude, speed, heading.
ITS-scuId	ITS-SCU-ID.
VciList	List containing information on all CIs and VCIs. Specified in Table 8.
CrossCiPrioList	Cross-CI prioritization list specified in Table 10.
TimerITSSI	Target period for transmission of a "ITSSI Data". Subject to temporary modifications by the congestion control.
ITS-scuList	ITS-SCU list specified in Table 7.
ITSSI	"ITSSI Data" of own station.
ApplReqList	Application requirement list specified in Table 11.
VCIperformList	VCI performance parameter list specified in Table 9.
Talive	Period of transmission of the "alive-signal" of an ITS-SCU.

Table C.1: Existing Management Parameters

ASN.1 Type	Valid Range	Description
Param24102.**itssi**		"ITSSI Data".
CM.**stationType**	"mobile", "fixed", "infrastructure", "unknown"	Specifying the type of station. "infrastructure" indicates possible access to fixed networks, e.g. Internet.
ITSSI.**stationID**	OCTET STRING	Identifier of ITS station, preferably globally unique.
ITSSI.**stationPosition**	KineVectOut	Kinemtics vector of station including timestamp specified in ISO 21218.

Table C.2: Parameters of ITS State Information (ITSSI)

ASN.1 Type	Valid Range	Description
Param24102.**applReqList**		Application requirement list used by CI selection manager.
ApplReqList.**applicationID**		Unique identifier of an ITS-S application / service in an ITS station.
ApplReqList.**requirements**		
.requirements.**dataRate**	See MI-parameter DataRateNW in ISO 21218.	Minimum average data rate requested at the IF-SAP in 100 bit/s. Corresponds with MI-parameter 6 in Table 9.
.requirements.**cost**	See MI-parameter Cost in ISO 21218.	Maximum acceptable cost of the link-usage in terms of money. Corresponds with MI-parameter 17 in Table 9.
.requirements.**nWsupport**	See MI-parameter NWsupport in ISO 21218.	Network protocol required.
.requirements.**medType**	See MI-parameter NedType in ISO 21218.	Type of CI required.

Table C.3: Parameters of *ApplReqList*

Table C.3 shows the parameters of *ApplReqList* specified in [ISO-24102-1-ITSS-management]. The parameters include the application requirements for the CI characteristics while the requirements for the path, which is the focus of the study, is missing. We need to extends ApplReqList to accommodates the needs for path selection, thus Flow requirement table is proposed in Section 6.1.3.

Table C.4 shows the parameters of the MF-Request function parameter called ITS-S-Appl-Reg. This is used to pass the application requirements from the facilities layer to the management entity. This function parameters also needs to be extended to adapt the flow requirement table.

Table C.5 and Table C.6 shows the existing MN-REQUEST and MN-COMMAND function parameters specified in [ISO-24102-1-ITSS-management].

ASN.1 Type	Valid Range	Description
MF-Request.**iTS-S-Appl-Reg**		Registration of a ITS-S application at the CI selection manager.
ITS-S-Appl-Reg.**applicationID**		Reference number of service application, unique in an ITS station.
.ApplicationID.**hostITS-ScuId**	ITS-scuId	ITS-SCU-ID of ITS-S host which contains service application.
.ApplicationID.**seqNumber**	0 - 65535	Sequential service application reference number, unique at ITS-SCU.
ITS-S-Appl-Reg.**requirements**	ApplRequirements	Requirements of the applications.
ITS-S-Appl-Reg.**socketID**	SocketID	Socket identifier containing IPv6 address and port number.
ITS-S-Appl-Reg.**physicalInfo**	PhysicalInfo	Properties of a CI.

Table C.4: ITS-S-Appl-Reg (MF-Request.No=0)

REQUEST name	Description
FWTsetNot	Notification of creation of an entry in a forwarding table.
FWTupdateNot	Notification of an update of an entry in a forwarding table.
FWTdeleteNot	Notification of deletion of an entry in a forwarding table.
VCIcreatePeerMAC	Request to create a VCI in a specific CI with a given relation to a peer station expressed by the MAC address of the peer station.
ItssiPeerNot	Notification of "ITSSI Data" from a peer station.
STArxNot	Notify reception of STA.
STCrxNot	Notify reception of STC.

Table C.5: Existing MN-REQUEST function parameters

COMMAND name	Description
FWTset	Sets an entry in the forwarding table of a networking protocol.
FWTupdate	Updates an entry in the forwarding table of a networking protocol.
FWTdelete	Deletes an entry in the forwarding table of a networking protocol.
GCperiodCmd	Send groupcast request to FAST networking protocol in order to trigger subsequent periodic groupcast transmissions to be performed by the FAST networking protocol.
GCstcTxCmd	Send "Service Table Context" (STC) to FAST networking protocol for the purpose of unicast delivery to the selected peer station.

Table C.6: Existing MN-COMMAND function parameters

List of Publications

Journals and Book chapters

1. Satoru Noguchi, Manabu Tsukada, Thierry Ernst, Astuo Inomata and Kazutoshi Fujikawa, "***Design and Field evaluation of geographical location-aware service discovery on IPv6 GeoNetworking for VANET***", special issue (SI) of "Network Routing and Communication Algorithm for Intelligent Transportation Systems" in EURASIP Journal on Wireless Communications and Networking. 2011.

2. Jong-Hyouk Lee, Manabu Tsukada, and Thierry Ernst, *"**MNPP: Mobile Network Prefix Provisioning for Enabling Route Optimization in Geographic Vehicular Networks**"*, Adhoc & Sensor Wireless Networks, 2011.

3. Manabu Tsukada, José Santa, Olivier Mehani, Yacine Khaled and Thierry Ernst, *"**Design and Experimental Evaluation of a Vehicular Network Based on NEMO and MANET**"*, The special issue for Vehicular Ad Hoc Networks, EURASIP Journal on Advances in Signal Processing, September 2010.

4. Yacine Khaled, Manabu Tsukada, José Santa and Thierry Ernst, *"**The Role of Communication Technologies in Vehicular Applications**"*, Book chapter 15, Advances in Vehicular Ad-Hoc Networks: Developments and Challenges, IGI Global (formerly Idea Group Inc.), April 2010

5. José Santa, Manabu Tsukada, Thierry Ernst, Olivier Mehani and Antonio F. Gómez-Skarmeta. *"**Assessment of VANET multi-hop routing over an experimental platform**"*, Int. J. Internet Protocol Technology, Vol. 4, No. 3, pp. 158-172, 2009 Inderscience Publishers, 2009

6. Yacine Khaled, Manabu Tsukada, José Santa, JinHyeock Choi and Thierry Ernst, *"**A usage oriented analysis of vehicular networks: from technologies to applications**"*, Journal of Communications (JCM, ISSN 1796-2021), Academy Publisher, Special Issue on Challenges in Future Vehicular AD HOC Networks, vol. 4, no. 5, pp. 357-368, May 2009

Conference and Workshop Papers

1. Satoru Noguchi, Manabu Tsukada, Thierry Ernst, Atsuo Inomata and Kazutoshi Fujikawa, ***"Location-aware service discovery on IPv6 GeoNetworking for VANET"***,

11th International Conference on Intelligent Transport System Telecommunications (ITST 2011), Saint-Petersburg, Russia, August 2011.

2. Thouraya Toukabri, Manabu Tsukada, Thierry Ernst and Lamjed Bettaieb, ***"Experimental evaluation of an open source implementation of IPv6 GeoNetworking in VANETs"***, 11th International Conference on Intelligent Transport System Telecommunications (ITST 2011), Saint-Petersburg, Russia, August 2011.

3. Satoru Noguchi, Manabu Tsukada, Ines Ben Jemaa and Thierry Ernst, ***"Real-vehicle integration of driver support application with IPv6 GeoNetworking"***, 2011 IEEE 73rd Vehicular Technology Conference (VTC2011-Spring), Budapest, Hungary, May 2011

4. Ines Ben Jemaa, Manabu Tsukada, Hamid Menouar and Thierry Ernst, ***"Validation and evaluation of NEMO in VANET using geographic routing"***, 10th International Conference on Intelligent Transport System Telecommunications (ITST 2010), Kyoto, Japan, November 2010.

5. Manabu Tsukada, Ines Ben Jemaa, Hamid Menouar, Wenhui Zhang, Maria Goleva and Thierry Ernst, ***"Experimental Evaluation for IPv6 over VANET Geographic routing"***, 6th International Wireless Communications and Mobile Computing Conference, IWCMC 2010, Caen, France, June 2010. (Best Paper Award)

6. Yacine Khaled, Manabu Tsukada and Thierry Ernst. ***"Geographical information extension for IPv6: application to VANET"***, 9th International Conference on Intelligent Transport System Telecommunications (ITST 2009), Lille, France, October 20, 2009.

7. Yacine Khaled, Ines Ben Jemaa, Manabu Tsukada and Thierry Ernst. ***"Application of IPv6 multicast to VANET"***, 9th International Conference on Intelligent Transport System Telecommunications (ITST 2009), Lille, France, October 20, 2009.

8. José Santa, Manabu Tsukada, Thierry Ernst and Antonio F. Gómez-Skarmeta. ***"Experimental Analysis of Multi-hop Routing in Vehicular Ad-hoc Networks"***, 2nd Workshop on Experimental Evaluation and Deployment Experiences on Vehicular networks (WEEDEV 2009) in conjunction with TRIDENTCOM 2009, Washington D.C., USA, April 6th, 2009.

9. Yacine Khaled, Manabu Tsukada, José Santa and Thierry Ernst. ***"On the Design of efficient Vehicular Applications"*** , 2009 IEEE 69th Vehicular Technology Conference (VTC2009-Spring), Barcelona, Spain, April 2009.

10. JinHyeock Choi, Yacine Khaled, Manabu Tsukada and Thierry Ernst. ***"IPv6 support for VANET with geographical routing"***, 8th International Conference on Intelligent Transport System Telecommunications (ITST 2008), Phuket, Thailand, October 22, 2008.

11. Nicolas Montavont, Antoine Boutet, Tanguy Ropitault, Manabu Tsukada, Thierry Ernst, Jari Korva, Cesar Viho and Laszlo Bokor. ***"Anemone: A ready-to-go testbed for IPv6 compliant Intelligent Transport Systems"***, 8th International Conference on Intelligent Transport System Telecommunications (ITST 2008), Phuket, Thailand, October 22, 2008.

12. Manabu Tsukada, Olivier Mehani and Thierry Ernst. ***"Simultaneous Usage of NEMO and MANET for Vehicular Communication"***, 1st Workshop on Experimental Evaluation and Deployment Experiences on Vehicular networks (WEEDEV 2008) conjonction with TRIDENTCOM 2008, Innsbruck, Austria, March 18, 2008.

Internet Drafts

1. Jong-Hyouk Lee, Manabu Tsukada and Thierry Ernst. ***"Mobile Network Prefix Provisioning"***, draft-jhlee-mext-mnpp-00.txt, Internet-Draft, IETF, October 2009.

Project Document Contributions

1. GeoNet project members, ***"D7.1 GeoNet Experimentation Results"***, GeoNet project deliverable, January, 2010
2. GeoNet project members, ***"D6.1 Porting and Integration Guideline"***, GeoNet project deliverable, January, 2010
3. GeoNet project members, ***"D3.1 Development Results"***, GeoNet project deliverable, January, 2010 (Project confidential)
4. GeoNet project members, ***"D2.2 Final GeoNet Specification"***, GeoNet project deliverable, January, 2010
5. Manabu Tsukada, Yacine Khaled and Thierry Ernst, ***"Basic and Advanced features of IPv6 Over C2C NET"***, GeoNet project internal report, July, 2009

Bibliography

[ABR] Chai-Keong Toh. Associativity-Based Routing for Ad Hoc Mobile Networks. *Wirel. Pers. Commun.*, 4(2):103–139, 1997. pages 35

[ACEA2008] ACEA. Motor vehicles in use in the enlarged eu. February 2008. http://www.acea.be/. pages 1

[Alshaer2009] H. Alshaer and J. Elmirghani. An intelligent route control scheme for multihomed mobile networks. In *Proc. IEEE 70th Vehicular Technology Conf. Fall (VTC 2009-Fall)*, pages 1–5, 2009. pages 45

[Balasubramanian2008] Aruna Balasubramanian, Ratul Mahajan, Arun Venkataramani, Brian Neil Levine, and John Zahorjan. Interactive wifi connectivity for moving vehicles. In *Proceedings of the ACM SIGCOMM 2008 conference on Data communication*, SIGCOMM '08, pages 427–438, New York, NY, USA, 2008. ACM. pages 47

[Balasubramanian2010] Aruna Balasubramanian, Ratul Mahajan, and Arun Venkataramani. Augmenting mobile 3g using wifi. In *Proceedings of the 8th international conference on Mobile systems, applications, and services*, MobiSys '10, pages 209–222, New York, NY, USA, 2010. ACM. pages 46

[BenRayana2009] R. Ben Rayana and J.-M. Bonnin. A smart management framework for multihomed mobile nodes & mobile routers. In *Proc. IEEE 20th Int Personal, Indoor and Mobile Radio Communications Symp*, pages 2881–2885, 2009. pages 45

[Bernardos2007] Carlos Jesus Bernardos, Ignacio Soto, María Calderón, Fernando Boavida, and Arturo Azcorra. Varon: Vehicular ad hoc route optimisation for nemo. *Computer Communications*, 30(8):1765–1784, 2007. pages 49

[C2C-CC-Manifesto2007] Car-to-Car Communication Consortium Manifesto (Overview of the C2C-CC System), August 2007. pages 14, 20, 24, 25

[CEDAR] Raghupathy Sivakumar, Prasun Sinha, and Vaduvur Bharghavan. *Core Extraction Distributed Ad hoc Routing (CEDAR) Specification*, October 1998. IETF, work in progress, draft-ietf-manet-cedar-spec-00. pages 35

[CGSR] Ching-Chuan Chiang, Hsiao-Kuang Wu, Winston Liu, and Mario Gerla. Routing in clustered multihop, mobile wireless networks with fading channel. In

IEEE Singapore International Conference on Networks, SICON'97, April 16-17, 1997, Singapore, pages 197–211. IEEE, IEEE, April 1997. pages 35

[COMeSafety-final] Information Society Technologies Specific Support Action COMeSafety Communication for eSafety. European its communication architecture overall framework proof of concept implementation. February 2010. http://www.comesafety.org/. pages 14, 21, 24, 25, 36

[CellularIP] András G. Valkó. Cellular IP: a new approach to Internet host mobility. *SIGCOMM Comput. Commun. Rev.*, 29(1):50–65, 1999. pages 43

[Columbia] John Ioannidis, Dan Duchamp, and Gerald Q. Maguire, Jr. IP-based protocols for mobile internetworking. In *SIGCOMM '91: Proceedings of the conference on Communications architecture & protocols*, pages 235–245, New York, NY, USA, 1991. ACM. pages 43

[DSDV] Charles E. Perkins and Pravin Bhagwat. Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers. *SIGCOMM Comput. Commun. Rev.*, 24(4):234–244, 1994. pages 35

[Dul2006] Andrew L. Dul. Global IP Network Mobility using Border Gateway Protocol (BGP). March 2006. The Boeing Company, white paper. pages 43

[E2E] Alex C. Snoeren and Hari Balakrishnan. An end-to-end approach to host mobility. In *MobiCom '00: Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 155–166, New York, NY, USA, 2000. ACM. pages 43

[EC-CARE-database2008] European Commission. EU | Road safety | CARE database | reports and graphics. 2008. http://ec.europa.eu/transport/road_safety/specialist/statistics/care_reports_graphics/. pages 1

[EC-COM-886:Action-plan] Action plan for the deployment of intelligent transport systems in europe, December 2008. COM(2008) 886 final. pages xiii, 2

[EC-M/453] Standardisation mandate addressed to cen, cenelec and etsi in the field of information and communication technologies to support the interoperability of co-operative systems for intelligent transport in the european community, October 2009. pages xiii, 2

[ETSI-EN-302-665-Arch] Intelligent Transport Systems (ITS); Communications Architecture, September 2010. ETSI EN 302 665 V1.1.1 (2010-09). pages xiv, 3, 21, 24, 25

[ETSI-EN-302-931-GeoArea] Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition, December 2010. Draft ETSI EN 302 931 V1.0.0 (2010-12). pages 94

[ETSI-TR-102-863-LDM] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Local Dynamic Map (LDM); Rationale for and guidance on standardization, June 2011. ETSI TR 102 863 V1.1.1 (2011-06). pages 23, 75, 76

[ETSI-TS-102-636-1-req] Intelligent Transportation Systems (ITS); Transport & Network; Vehicular Communications; Part 1: Requirements for GeoNetworking and Data Transport Protocol, March 2010. ETSI TS 102 636-1 V1.1.1 (2010-03). pages 23, 36

[ETSI-TS-102-636-2-Scenario] Intelligent Transportation Systems (ITS); Transport & Network: Vehicular Communications; GeoNetworking and Data Transport; Part 2: Scenarios for GeoNetworking, March 2010. ETSI TS 102 636-2 V1.1.1 (2010-03). pages 23, 36

[ETSI-TS-102-636-3-GeoNetworking-Arch] Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 3: Network architectures, March 2010. ETSI TS 102 636-3 V1.1.1 (2010-03). pages 22, 23, 115, 201

[ETSI-TS-102-636-4-1-Media] Intelligent Transport Systems (ITS); Vehicular Communications; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-part 1: Media-Independent Functionality, June 2011. ETSI TS 102 636-4-1 V1.1.1 (2011-06). pages 23, 36, 92

[ETSI-TS-102-636-4-2-Media] Intelligent Transportation Systems (ITS); Vehicular Communications; Part 4: Geographical Addressing and Forwarding for Point-to-Point and Point-to-Multipoint Communications; Sub-part 2: Media-Dependent Functionalities for ITS-G5A media, May 2010. ETSI, work in progress, ETSI-TS-102-636-4-2. pages 23, 36

[ETSI-TS-102-636-5-1-Transport] Intelligent Transport Systems (ITS); Vehicular Communications; Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocols, February 2011. ETSI TS 102 636-5-1 V1.1.1 (2011-02). pages 23

[ETSI-TS-102-636-6-1-IPv6-GeoNetworking] Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols, March 2011. ETSI TS 102 636-6-1 V1.1.1 (2011-03). pages 22, 23, 115, 201

[ETSI-TS-102-637-2-CAM] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service, March 2011. ETSI TS 102 637-2 V1.2.1 (2011-03). pages 23, 76

[ETSI-TS-102-637-3-DENM] Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification (DENM) Basic Servic, September 2010. ETSI TS 102 637-3 V1.1.1 (2010-09). pages 23, 76

[ElBatt2006] Tamer ElBatt, Siddhartha K. Goel, Gavin Holland, Hariharan Krishnan, and Jayendra Parikh. Cooperative collision warning using dedicated short range wireless communications. In *VANET '06: Proceedings of the 3rd international workshop on Vehicular ad hoc networks*, pages 1–9, New York, NY, USA, 2006. ACM. pages 31

[FHWA1996] United States Department of Transportation (Federal Highway Administration). Intelligent transportation systems in japan - vol. 60Â· no. 2 - public

roads. page http://www.fhwa.dot.gov/publications/publicroads/96fall/p96au41.cfm, 1996. pages xiii, 2

[Fazio2006] F. Fazio, C. Palazzi, S. Das, and M. Gerla. *Automatic IP Address Configuration in VANETs*, 2006. ACM VANET 2006 Workshop co-located with Mobicom 2006. pages 39

[Fishburn1967] P. C. Fishburn. Additive utilities with incomplete product set: Applications to priorities and assignments. *American Society of Operations Research (ORSA)*, 1967. pages 87

[Flstad2009] E. L. Flstad and B. E. Helvik. Managing availability in wireless inter domain access. In *Proc. Int. Conf. Ultra Modern Telecommunications & Workshops ICUMT '09*, pages 1–6, 2009. pages 45

[Funding-FP6] European Union. Decision no 786/2004/ec of the european parliament and of the council of 21 april 2004. *Official Journal of the European Union*, April 2004. pages 18

[Funding-FP7] COUNCIL OF THE EUROPEAN UNION. Council approves eu research programmes for 2007-2013. December 2006. pages 18

[GeoNet-D.1] Thierry Ernst, Carlos J. Bernardos, Maria Calderon, JinHyeock Choi, Yacine Khaled, Andras Kovacs, Massimiliano Lenardi, Wilfried Lohmann, Hamid Menouar, Carsten Schulze, and Wenhui Zhang. GeoNet STREP No. 216269 D1.2 Final GeoNet Architecture Design. 2010. GeoNet-D.1.2-v1.1. pages 20, 24, 25, 28

[GeoNet-D.2] Thierry Ernst, Andras Kovacs, Carlos J. Bernardos, Carsten Schulze, Hamid Menouar, Ines Ben Jemaa, JinHyeock Choi, Jong-Hyouk Lee, Manabu Tsukada, Marco Gramaglia, Maria Calderon, Massimiliano Lenardi, Wenhui Zhang, Wilfried Lohmann, and Yacine Khaled. GeoNet STREP No. 216269 D2.2 Final GeoNet Specification. January 2010. GeoNet-D.2.2-v1.1. pages 36, 37, 40, 115, 200

[GeoNet-D.3] Carsten Schulze, Hamid Menouar, Jong-Hyouk Lee, Manabu Tsukada, Marco Gramaglia, Maria Goleva, and Wenhui Zhang. GeoNet STREP No. 216269 D3.1 Development Results. 2010. GeoNet-D3.1-v1.0 (Project Confidential). pages xviii, 10, 127, 201

[GeoNet-D.6] Carsten Schulze, Hamid Menouar, Jong-Hyouk Lee, Manabu Tsukada, Marco Gramaglia, Maria Goleva, and Wenhui Zhang. GeoNet STREP No.216269 D6.1 Porting and Integration Guideline. 2010. GeoNet-D6.1-v1.0. pages 201

[GeoNet-D.7] Thierry Ernst, Maria Goleva, Ines Ben Jemaa, Andras Kovacs, Hamid Menouar, Satoru Noguchi Carsten Schulze, Manabu Tsukada, Philippe Zhang, and Wenhui Zhang. GeoNet STREP No.216269 D7.1 GeoNet Experimentation Results. 2010. GeoNet-D7.1-ExperimentationResults-v1.0. pages 148, 149, 186, 201

[Gustafsson2003] E. Gustafsson and A. Jonsson. Always best connected. 10(1):49–55, 2003. pages 45

[HAWAII] R. Ramjee, K. Varadhan, L. Salgarelli, S.R. Thuel, Shie-Yuan Wang, and T. La Porta. HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks. *Networking, IEEE/ACM Transactions on*, 10(3):396 –410, jun. 2002. pages 43

[Hartenstein2008] H. Hartenstein and K. P. Laberteaux. A tutorial survey on vehicular ad hoc networks. 46(6):164–171, June 2008. pages 35

[Hattori2004] G. Hattori, C. Ono, S. Nishiyama, and H. Horiuchi. Implementation and evaluation of message delegation middleware for its application. In *Proc. SAINT 2004 Workshops Applications and the Internet Workshops 2004 Int. Symp*, pages 326–333, 2004. pages 31

[Hu2008] Xin Hu, Li Li, Z. M. Mao, and Y. R. Yang. Wide-Area IP Network Mobility. In *Proc. INFOCOM 2008. The 27th Conf. Computer Communications. IEEE*, pages 951–959, 2008. pages 43

[IEEE-1609.0-Arch] IEEE 1609.0 Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Architecture, April 2010. pages 15

[IEEE-1609.1-RemoteMNG] IEEE 1609.1 D1.3 Draft Standard for Wireless Access in Vehicular Environments (WAVE) Remote Management Services, May 2010. pages 16

[IEEE-1609.11-Payment] IEEE 1609.11-2011: Standard for Wireless Access in Vehicular Environments (WAVE) – Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transportation Systems (ITS), Jan 2011. pages 16

[IEEE-1609.2-Security] IEEE 1609.2-2006: Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, 2006. pages 16

[IEEE-1609.3-Networking] IEEE 1609.3-2010: Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, December 2010. pages 16

[IEEE-1609.4-MultiChannel] IEEE 1609.4/D9: Draft Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation, August 2010. pages 16

[IEEE-802.2-LLC] IEEE Std 802.2, 1998 Edition(R2003) - IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 2 Logical Link Control, May 1998. pages 16

[IEEE802-11-2007] IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks-Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 2007. pages 16

[IEEE802-11a] Supplement to IEEE standard for information technology - telecommunications and information exchange between systems - local and metropolitan area networks - specific requirements. Part 11: wireless LAN Medium Access Control (MAC) and Physical Layer (PHY), 1999. IEEE Std 802.11a-1999. pages 31

[IEEE802-11b] Supplement to IEEE 802.11-1999,Wireless LAN MAC and PHY specifications: Higher speed Physical Layer (PHY) extension in the 2.4 GHz band, 1999. IEEE Std 802.11b-1999. pages 31

[IEEE802-11g] IEEE 802.11g-2003 IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications - Amendment 4: Further Higher-Speed Physical Layer Extension in the 2.4 GHz Band, 2003. IEEE Std 802.11g-2003. pages 31

[IEEE802-11p] IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirement, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, July 2010. IEEE Std 802.11p-2010. pages 16, 20, 26, 27, 31

[IEEE802-15-1-bluetooth] IEEE Std 802.15.1 IEEE Standard for Information technology-Telecommunications and information exchange between systems- Local and metropolitan area networks- Specific requirements Part 15.1: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Wireless Personal Area Networks (WPANs), 2002. pages 31

[IEEE802-16-2009] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems, May 2009. pages 32

[IEEE802-16e] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment for Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands., 2005. IEEE Std 802.16e-2005. pages 32

[ILNPv6] Ran Atkinson, Saleem Bhatti, and Stephen Hailes. A proposal for unifying mobility with multi-homing, NAT, & security. In *MobiWac '07: Proceedings of the 5th ACM international workshop on Mobility management and wireless access*, pages 74–83, New York, NY, USA, 2007. ACM. pages 43

[ISO-21210:2011-CALM-IPv6] ISO/DIS 21210.2 Intelligent transport systems – Communications access for land mobiles (CALM) – IPv6 Networking, January 2011. ISO 21210:2011(E). pages 3, 22, 58, 59, 117

[ISO-21217-CALM-Arch] ISO 21217:2010 Intelligent transport systems – Communications access for land mobiles (CALM) – Architecture, April 2010. pages xiv, 3, 21, 24, 25, 26

[ISO-21218:2008-CALM-Medium-SAP] ISO 21218:2008 Intelligent transport systems – Communications access for land mobiles (CALM) – Medium service access points, August 2008. pages 21, 77, 78, 96, 107, 245

[ISO-24102-1-ITSS-management] ISO/CD 24102-1 Intelligent transport systems – Communications access for land mobiles (CALM) – Part 1: ITS station management, May 2011. pages 65, 75, 78, 80, 215, 217

[ISO-24102-2-Management-SAP] ISO/CD 24102-2 Intelligent transport systems – Communications access for land mobiles (CALM) – Part 2: Management service access points, May 2011. pages 77, 90, 95, 96, 98, 107, 108, 215

[ISO-24102-4-FSAP] ISO/CD 24102-4 Intelligent transport systems – Communications access for land mobiles (CALM) – Part 4: Fast service advertisement protocol (FSAP), May 2011. pages 23

[ISO-24102-CALM-Management] ISO/FDIS 24102 Intelligent transport systems – Communications access for land mobiles (CALM) – Management, September 2010. pages 24, 65, 75, 80, 96

[ISO-29281-CALM-non-IP] ISO 29281:2011 Intelligent transport systems – Communications access for land mobiles (CALM) – Non-IP networking, March 2011. pages 22

[ITU-T-X.680-ASN1:2002] Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation, July 2002. ITU-T Rec. X.680 ISO/IEC 8824-1. pages 90

[Ines2010] Ben Jemaa Ines, Manabu Tsukada, Hamid Menouar, and Thierry Ernst. Validation and evaluation of nemo in vanet using geographic routing. In *Proc. 10th International Conference on ITS Telecommunications ITST 2010*, November 2010. pages xviii, 10, 127, 186, 201

[Intelligent-Car-Initiative2006] On the Intelligent Car Initiative "Raising Awareness of ICT for Smarter, Safer and Cleaner Vehicles". Communication from the commission to the council, the european parliament, the european economic and social committee and the committee of the regions. 2006. pages 1, 18

[JAMA2009] Inc Japan Automobile Manufacturers Association (JAMA). The motor industry of japan 2009. May 2009. http://www.jama-english.jp/publications/MIJ2009.pdf. pages 1, 2

[JRC-IPTS2009] JRC-IPTS. The 2009 report on r&d in ict n the european union. 2009. http://ftp.jrc.es/EURdoc/JRC49951.pdf. pages 2

[Karp2000] Brad Karp and H. T. Kung. Gpsr: Greedy perimeter stateless routing for wireless networks. In *6th Annual International Conference on Mobile Computing and Networking, MobiCom 2000, August 6.-11., 2000, Boston, Massachusetts, USA*, pages 243–254. ACM / IEEE, August 2000. pages 35, 36

[Khaled2010] Yacine Khaled, Manabu Tsukada, José anta, and Thierry Ernst. The role of communication and network technologies in vehicular applications. In *Book chapter 15, Advances in Vehicular Ad-Hoc Networks: Developments and Challenges*. IGI Global (formerly Idea Group Inc.), 2010. pages 30

[Khaleda2009] Yacine Khaleda, Manabu Tsukada, Jose Santa, JinHyeock Choi, and Thierry Ernst. A usage oriented analysis of vehicular networks: from technologies to applications. *Journal of Communications (JCM, ISSN 1796-2021), Academy Publisher, Special Issue on Challenges in Future Vehicular AD HOC Networks*, May 2009. pages 30

[Ko1999] Y. B. Ko and N. H. Vaidya. Geocasting in mobile ad hoc networks: location-based multicast algorithms. In *Proc. Second IEEE Workshop on Mobile Computing Systems and Applications WMCSA '99*, pages 101–110, 25–26 Feb. 1999. pages 35

[Kuntz2008a] Romain Kuntz, Julien Montavont, and Thomas Noel. Multiple mobile routers in nemo: How neighbor discovery can assist default router selection. In *Proc. IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications PIMRC 2008*, pages 1–6, 15–18 Sept. 2008. pages 45

[LIN6] Masahiro Ishiyama Mitsunobu Kunishi, Keisuke Uehara, Hiroshi Esaki, and Fumio Teraoka. Lin6: A new approach to mobility support in ipv6. In *Proceedings of the Third Inernational Sympsium on Wireless Personal Multimedia Communications*, November 2000. pages 43

[LSR] Pravin Bhagwat and Charles E. Perkins. A mobile networking system based on internet protocol(IP). In *MLCS: Mobile & Location-Independent Computing Symposium on Mobile & Location-Independent Computing Symposium*, pages 7–7, Berkeley, CA, USA, 1993. USENIX Association. pages 43

[Lee2011] Jong-Hyouk Lee, Manabu Tsukada, and Thierry Ernst. MNPP: Mobile Network Prefix Provisioning for Enabling Route Optimization in Geographic Vehicular Networks. In *Adhoc & Sensor Wireless Networks*, 2011. pages 40

[Lorchat2006d] Jean Lorchat and Keisuke Uehara. Optimized inter-vehicle communications using nemo and manet. In *Proc. Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services*, pages 1–6, July 2006. pages 48, 51

[M-SCTP] Wei Xing, Holger Karl, Adam Wolisz, and Harald MÃŒller. M-SCTP: Design And Prototypical Implementation Of An End-To-End Mobility Concept. In *In Proc. 5th Intl. Workshop The Internet Challenge: Technology and Applications*, 2002. pages 43

[MSM-IP] Jayanth Mysore and Vaduvur Bharghavan. A new multicasting-based architecture for Internet host mobility. In *MobiCom '97: Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking*, pages 161–172, New York, NY, USA, 1997. ACM. pages 43

[Maihfer04] C. Maihfer. A Survey of Geocast Routing Protocols. *IEEE Communications Surveys and Tutorials*, 6, 2nd quarter 2004. pages 36

[Mauve2001] M. Mauve, A. Widmer, and H. Hartenstein. A survey on position-based routing in mobile ad hoc networks. 15(6):30–39, 2001. pages 35

[Mitsuya2007] Koshiro Mitsuya, Romain Kuntz, Shinta Sugimoto, Ryuji Wakikawa, and Jun Murai. A policy management framework for flow distribution on multihomed end nodes. In *MobiArch '07: Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture*, pages 1–7, New York, NY, USA, 2007. ACM. pages 48

[Montavont2008a] Nicolas Montavont, Antoine Boutet, Tanguy Ropitault, Manabu Tsukada, Thierry Ernst, Jari Korva, Cesar Viho, and Laszlo Bokor. Anemone: A ready-to-go testbed for ipv6 compliant intelligent transport systems. In *Proc. 8th International Conference on ITS Telecommunications ITST 2008*, pages 228–233, 24–24 Oct. 2008. pages 201

[Murthy2004] C. Siva Ram Murthy and B. S. Manoj. Ad Hoc Wireless Networks - Architectures and Protocols. In *Pearson/Prentice Hall*, May 2004. ISBN: 0-13-147023-X. pages 33

[Ng2004] Chan-Wah Ng and T. Ernst. Multiple access interfaces for mobile nodes and networks. In *Proc. 12th IEEE Int. Conf. Networks (ICON 2004)*, volume 2, pages 774–779, 2004. pages 45

[Noguchi2011] Satoru Noguchi, Manabu Tsukada, Ines Ben Jemaa, and Thierry Ernst. Real-Vehicle Integration of Driver Support Application with IPv6 GeoNetworking. In *Proc. IEEE 73rd Vehicular Technology Conf. (VTC Spring)*, pages 1–5, 2011. pages 201

[Paik2004] Eun Kyoung Paik, Ho sik Cho, T. Ernst, and Yanghee Choi. Load sharing and session preservation with multiple mobile routers for large scale network mobility. In *Proc. 18th International Conference on Advanced Information Networking and Applications AINA 2004*, volume 1, pages 393–398, 2004. pages 45

[Paik2004a] Eun Kyoung Paik, Hosik Cho, Taekyoung Kwon, and Yanghee Choi. Mobility-aware mobile router selection and address management for ipv6 network mobility. *J. Netw. Syst. Manage.*, 12(4):485–505, 2004. pages 45

[Paik2008b] Eun Kyoung Paik, Hosik Cho, Thierry Ernst, and Yanghee Choi. Load sharing and session preservation with multiple mobile routers for large scale mobile networks. *Int. J. Wire. Mob. Comput.*, 3(1/2):56–68, 2008. pages 45

[RAYANA2010] Rayene BEN RAYANA. *A smart management framework for multihomed mobile nodes & mobile routers*. PhD thesis, Télécom bretagne, 2010. pages 45

[Rao2007] R. Venkata Rao. Introduction to decision making in the manufacturing environment. In *Decision Making in the Manufacturing Environment*, Springer Series in Advanced Manufacturing, pages 3–6. Springer London, 2007. 10.1007978-1-84628-819-7_1. pages 86

[Ronan2008] John Ronan, Sasitharan Balasubramaniam, Adnan K Kiani, and Wenbing Yao. On the use of shim6 for mobility support in ims networks. In *TridentCom '08: Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*, pages 1–6, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). pages 44

[Ropitault2008] T. Ropitault and N. Montavont. Implementation of flow binding mechanism. In *Proc. Sixth Annual IEEE International Conference on Pervasive Computing and Communications PerCom 2008*, pages 342–347, 17–21 March 2008. pages 48

[SAE-J2735-DSRC-Message-Set] SAE J2735 Dedicated Short Range Communications (DSRC) Message Set Dictionary, November 2009. pages 16

[Santa2009a] José Santa, Manabu Tsukada, Thierry Ernst, Olivier Mehani, and F. Gómez-Skarmeta. Assessment of vanet multi-hop routing over an experimental platform. In *Int. J. Internet Protocol Technology*, volume Vol. 4. Inderscience Publishers, 2009. pages 148, 149, 173, 201

[Santa2009b] J. Santa, M. Tsukada, T. Ernst, and A. F. Gomez-Skarmeta. Experimental analysis of multi-hop routing in vehicular ad-hoc networks. In *Proc. 5th International Conference on Testbeds and Research Infrastructures for the Development of Networks. Communities and Workshops TridentCom 2009*, pages 1–8, April 6–8, 2009. pages 148, 149, 173, 201

[Satoru2011] Noguchi Satoru, Manabu Tsukada, Thierry Ernst, Atsuo Inomata, and Kazutoshi Fujikawa. Location-aware service discovery on IPv6 GeoNetworking for VANET. In *ITST 2011 : 11th International Conference on Intelligent Transport System Telecommunications*, Saint-Petersburg, Russie, Fédération De, August 2011. Conference is technically co-sponsored by IEEE Communications Society and co-organized by the Technical Sub-Committee on Vehicular Networks and Telematics (VNAT). pages 149

[Srinivasan2008] Kannan Srinivasan, Maria A. Kazandjieva, Saatvik Agarwal, and Philip Levis. The beta-factor: measuring wireless link burstiness. In Tarek F. Abdelzaher, Margaret Martonosi, and Adam Wolisz, editors, *SenSys*, pages 29–42. ACM, 2008. pages 47

[Sun2006] Weihua Sun, H. Yamaguchi, and S. Kusumoto. A study on performance evaluation of real-time data transmission on vehicular ad hoc networks. In *Proc. 7th International Conference on Mobile Data Management MDM 2006*, pages 126–126, 10–12 May 2006. pages 36

[Sun2006a] W. Sun, H. Yamaguchi, K. Yukimasa, and S. Kusumoto. Gvgrid: A qos routing protocol for vehicular ad hoc networks. In *Proc. 14th IEEE International Workshop on Quality of Service IWQoS 2006*, pages 130–139, 19–21 June 2 2006. pages 36

[TIMIP] A. Grilo, P. Estrela, and M. Nunes. Terminal independent mobility for IP (TIMIP). *Communications Magazine, IEEE*, 39(12):34 –41, dec. 2001. pages 43

[TORA] V. Park and S. Corson. *Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification*, July 2001. IETF, Work in progress, draft-ietf-manet-tora-spec-04. pages 35

[Teraoka1991] Fumio Teraoka, Yasuhiko Yokore, and Mario Tokoro. A network architecture providing host migration transparency. *SIGCOMM Comput. Commun. Rev.*, 21(4):209–220, 1991. pages 43

[Toukabri2011] Thouraya Toukabri, Manabu Tsukada, Thierry Ernst, and Lamjed Bettaieb. Experimental evaluation of an open source implementation of IPv6 GeoNetworking in VANETs. In *ITST 2011 : 11th International Conference on Intelli-*

gent Transport System Telecommunications, Saint-Petersburg, Russie, Fédération De, August 2011. Conference is technically co-sponsored by IEEE Communications Society and co-organized by the Technical Sub-Committee on Vehicular Networks and Telematics (VNAT). pages xviii, xix, 10, 11, 127, 149, 188, 201

[Tsukada2005] M. Tsukada, T. Ernst, R. Wakikawa, and K. Mitsuya. Dynamic management of multiple mobile routers. In *Proc. 13th IEEE International Conference on Networks Jointly held with the 2005 IEEE 7th Malaysia International Conference on Communication*, volume 2, page 6pp., 16–18 Nov. 2005. pages 45

[Tsukada2008] Manabu Tsukada, Olivier Mehani, and Thierry Ernst. Simultaneous usage of NEMO and MANET for vehicular communication. In *TridentCom '08: Proceedings of the 4th International Conference on Testbeds and research infrastructures for the development of networks & communities*, pages 1–8, ICST, Brussels, Belgium, Belgium, 2008. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering). pages xviii, 10, 48, 51, 127, 173, 201

[Tsukada2009] Manabu Tsukada, Yacine Khaled, and Thierry Ernst. Basic and Advanced features of IPv6 Over C2C NET. GeoNet Project internal report (confidential at 2009), July 2009. http://hal.inria.fr/inria-00565574/en/. pages 115, 201

[Tsukada2010a] Manabu Tsukada, José Santa, Olivier Mehani, Yacine Khaled, and Thierry Ernst. Design and Experimental Evaluation of a Vehicular Network Based on NEMO and MANET. In *The special issue for Vehicular Ad Hoc Networks, EURASIP Journal on Advances in Signal Processing*, 2010. pages xviii, 10, 127, 173, 201

[Tsukada2010b] Manabu Tsukada, Ines Ben Jemaa, Hamid Menouar, Wenhui Zhang, Maria Goleva, and Thierry Ernst. Experimental evaluation for IPv6 over VANET geographic routing. In *IWCMC '10: Proceedings of the 6th International Wireless Communications and Mobile Computing Conference*, pages 736–741, New York, NY, USA, 2010. ACM. pages xviii, 10, 115, 127, 148, 149, 186, 201

[WHO2004] WHO | World Health Organization. World report on road traffic injury prevention. 2004. http://www.who.int/violence_injury_prevention/publications/road_traffic/world_report/. pages 1

[WHO2008] WHO | World Health Organization. The global burden of disease : 2004 update. 2008. http://www.who.int/healthinfo/global_burden_disease/. pages 1

[WRP] Shree Murthy and J. J. Garcia-Luna-Aceves. An efficient routing protocol for wireless networks. *Mob. Netw. Appl.*, 1(2):183–197, 1996. pages 35

[Wakikawa2003] R. Wakikawa, S. Koshiba, K. Uehara, and J. Murai. Orc: optimized route cache management protocol for network mobility. In *Proc. 10th International Conference on Telecommunications ICT 2003*, volume 2, pages 1194–1200, 23 Feb.–1 March 2003. pages 50

[Wakikawa2005a] Ryuji Wakikawa, Kouji Okada, Rajeev Koodli, and Anders Nilsson. Design of vehicle network: mobile gateway for MANET and NEMO converged communication. In *VANET '05: Proceedings of the 2nd ACM international workshop on Vehicular ad hoc networks*, pages 81–82, New York, NY, USA, 2005. ACM. pages 48, 51

[Watari2006] M. Watari, T. Ernst, and R. Wakikawa. *Routing Optimization for Nested Mobile Networks*, October 2006. IEICE Trans. Commun. (IEICE) Volume E89-B, Issue 10. pages 50

[ZHLS] Mario Joa-Ng. *Routing Protocol and Medium Access Protocol for Mobile Ad Hoc Networks*. PhD thesis, Polytechnic University, NY, USA, January 1999. pages 35

[ZRP] Zygmunt J. Haas, Marc R. Pearlman, and Prince Samar. *The Zone Routing Protocol (ZRP) for Ad Hoc Networks*, July 2002. IETF work in progress, draft-ietf-manet-zone-zrp-04. pages 35

[draft-bernardos-autoconf-evaluation-considerations] H. Moustafa, C. Bernardos, and M. Calderon. Evaluation considerations for ip autoconfiguration mechanisms in manets, November 2, 2008 2008. Work in Progress, draft-bernardos-autoconf-evaluation-considerations-03. pages 34, 39

[draft-bernardos-manet-autoconf-survey] C. Bernardos, M. Calderon, and H. Moustafa. Survey of ip address autoconfiguration mechanisms for manets, June 2010. Work in Progress, draft-bernardos-manet-autoconf-survey-05. pages 34, 39

[draft-bernardos-mext-nemo-ro-cr] C. Bernardos, M. Calderon, and I. Soto. Correspondent router based route optimisation for nemo (cron), July 2008. Work in Progress, draft-bernardos-mext-nemo-ro-cr-00. pages 50

[draft-cha-manet-extended-support-globalv6] A. Laouiti. Extended support for global connectivity for ipv6 mobile ad hoc networks, October 2003. Work in Progress, draft-cha-manet-extended-support-globalv6-00. pages 39

[draft-clausen-manet-address-autoconf] T. Clausen and E. Baccelli. Simple manet address autoconfiguration, February 2005. IETF, draft-clausen-manet-address-autoconf-00. pages 39

[draft-eriksson-mext-mipv6-routing-rules] M. Eriksson, C. Larsson, and R. Kuntz. *Mobile IPv6 Flow Routing over Multiple Care-of Addresses*. IETF, June 2008. Work in progress, draft-eriksson-mext-mipv6-routing-rules-00. pages 48

[draft-haley-mext-generic-notification-message] Brian Haley and Sri Gundavelli. *Generic Notification Message for Mobile IPv6*. IETF, April 2008. Work in progress, draft-haley-mext-generic-notification-message-00. pages 48

[draft-hofmann-autoconf-mran] P. Hofmann. Multihop radio access network (mran) protocol specification, March 2006. IETF, draft-hofmann-autoconf-mran-00. pages 39

[draft-ietf-autoconf-manetarch] I. Chakeres, J. Macker, and T. Clausen. Mobile ad hoc network architecture, November 2008. Work in Progress, draft-ietf-autoconf-manetarch-07. pages 39

[draft-ietf-autoconf-statement] E. Baccelli. Address autoconfiguration for manet: Terminology and problem statement, February 2008. Work in Progress, draft-ietf-autoconf-statement-04. pages 39

[draft-ietf-mext-nemo-ro-automotive-req] R. Baldessari, T. Ernst, A. Festag, and M. Lenardi. *Automotive Industry Requirements for NEMO Route Optimization*. IETF, January 2009. Work in progress, draft-ietf-mext-nemo-ro-automotive-req-02. pages 48

[draft-ietf-monami6-mipv6-analysis] N. Montavont, R. Wakikawa, T. Ernst, C. Ng, and K. Kuladinithi. *Analysis of Multihoming in Mobile IPv6*, May 2008. IETF, work in progress, draft-ietf-monami6-mipv6-analysis-05. pages 44

[draft-ietf-monami6-multihoming-motivation-scenario] T. Ernst, N. Montavont, R. Wakikawa, C. Ng, and K. Kuladinithi. *Motivations and Scenarios for Using Multiple Interfaces and Global Addresses*, May 2008. IETF, work in progress, draft-ietf-monami6-multihoming-motivation-scenario-03. pages 44

[draft-jeong-nemo-ro-ndproxy] J. Jeong, K. Lee, and H. Kim. *ND-Proxy based Route and DNS Optimizations for Mobile Nodes in Mobile Network*, February 2004. IETF Work in progress, draft-jeong-nemo-ro-ndproxy-02. pages 51

[draft-jhlee-mext-mnpp] Jong-Hyouk Lee, Manabu Tsukada, and Thierry Ernst. Mobile network prefix provisioning (mnpp), October 2009. IETF, Work in progress, draft-jhlee-mext-mnpp-00. pages 40

[draft-laouiti-manet-olsr-address-autoconf] A. Laouiti. Address autoconfiguration in optimized link state routing protocol, July 2005. IETF, draft-laouiti-manet-olsr-address-autoconf-01. pages 39

[draft-larsson-mext-flow-distribution-rules] C. Larsson, M. Eriksson, K. Mitsuya, K. Tasaka, and R. Kuntz. *Flow Distribution Rule Language for Multi-Access Nodes*. IETF, February 2009. Work in progress, draft-larsson-mext-flow-distribution-rules-02. pages 48, 103

[draft-leekj-nemo-ro-pd] K. Lee, J. Jeong, J. Park, and H. Kim. *Route Optimization for Mobile Nodes in Mobile Network based on Prefix Delegation*, February 2004. IETF Work in progress, draft-leekj-nemo-ro-pd-02. pages 51

[draft-mccarthy-manemo-configuration-problems] B. McCarthy, A. Petrescu, and T. H. Clausen. *MANEMO Configuration Problems (MCP)*, March 2007. IETF, draft-mccarthy-manemo-configuration-problems-00. pages 51

[draft-meyer-lisp-mn] D. Farinacci, D. Lewis, D. Meyer, and C. White. *LISP Mobile Nodes*, October 2011. IETF, Work in Progress, draft-meyer-lisp-mn-06. pages 43

[draft-na-nemo-nested-path-info] J. Na, S. Cho, C. Kim, S. Lee, H. Kand, and C. Koo. *Secure Nested Tunnels Optimization using Nested Path Information*, September 2003. IETF, draft-na-nemo-nested-path-info-00. pages 51

[draft-na-nemo-path-control-header] J. Na, S. Cho, C. Kim, S. Lee, H. Kand, and C. Koo. *Route Optimization Scheme based on Path Control Header*, April 2004. IETF, draft-na-nemo-path-control-header-00. pages 50

[draft-ng-nemo-access-router-option] C. Ng and J. Hirano. *Securing Nested Tunnels Optimization with Access Router Option*, July 2004. IETF, draft-ng-nemo-access-router-option-01. pages 51

[draft-perera-nemo-extended] E. Perera, R. Hsieh, and A. Seneviratne. *Extended Network Mobility Support*, July 2003. IETF Work in Progress, draft-perera-nemo-extended-00. pages 51

[draft-petrescu-autoconf-ra-based-routing] A. Petrescu and C. Janneteau. Router Advertisements for Routing between Moving Networks, July 2010. IETF, Work in progress, draft-petrescu-autoconf-ra-based-routing-00. pages 40

[draft-ros-autoconf-emap] P. Ruiz and F. Ros. Extensible manet auto-configuration protocol (emap), March 2006. Work in Progress, draft-ros-autoconf-emap-02. pages 39

[draft-ruffino-manet-autoconf-multigw] S. Ruffino and P. Stupar. Automatic configuration of ipv6 addresses for manet with multiple gateways (amg), June 2006. Work in Progress, draft-ruffino-manet-autoconf-multigw-03. pages 39

[draft-thubert-nemo-global-haha] P. Thubert, R. Wakikawa, and V. Devarapalli. *Global HA to HA protocol*, September 2006. IETF, draft-thubert-nemo-global-haha-02. pages 50

[draft-thubert-nemo-reverse-routing-header] P. Thubert and M. Molteni. *IPv6 Reverse Routing Header and its application to Mobile Networks*, February 2007. IETF, draft-thubert-nemo-reverse-routing-header-07. pages 51

[draft-wakikawa-manemo-problem-statement] R. Wakikawa, P. Thubert, T. Boot, J. Bound, and B. McCarthy. Problem statement and requirements for manemo, July 2007. Work in Progress, draft-wakikawa-manemo-problem-statement-01. pages 48, 51

[draft-wakikawa-manemoarch] R. Wakikawa, T. Clausen, B. McCarthy, and A. Petrescu. Manemo topology and addressing architectures, July 2007. Work in Progress, draft-wakikawa-manemoarch-00. pages 48, 51

[draft-wakikawa-manet-globalv6] Ryuji Wakikawa, Jari T. Malinen, Charles E. Perkins, Anders Nilsson, and Antti J. Tuominen. Global connectivity for ipv6 mobile ad hoc networks, March 2006. Work in Progress, draft-wakikawa-manet-globalv6-05. pages 39

[draft-wakikawa-mext-cr-consideration] R. Wakikawa. *The Design Consideration of Correspondent Router*. IETF, July 2008. Work in progress, draft-wakikawa-mext-cr-consideration-00. pages 50

[dsrc] *Dedicated Short-Range Communication - Physical layer using microwave at 5.8 GHz (review)*, July 2004. EN 12253:2004. pages 31

[dymo] I. Chakeres and C. Perkins. *Dynamic MANET On-demand (DYMO) Routing*, July 2010. IETF, draft-ietf-manet-dymo-21. pages 35

[eSafety2003] COMMISSION OF THE EUROPEAN COMMUNITIES. Information and Communications Technologies for Safe and Intelligent Vehicles. 2003. pages 18

[i2010] i2010 A European Information Society for growth and employment. Europe's digital competitiveness report main achievements of the i2010 strategy 2005-2009. August 2009. http://ec.europa.eu/information_society/eeurope/i2010/. pages 2

[liao00] W-H. Liao, Y-C. Tseng, K-L. Lo, and J-P. Sheu. Geogrid: a Geocasting Protocol for Mobile Ad Hoc Networks based on Grid. *Journal of Internet Technology*, 1:23–32, 2000. pages 36

[manetwg] IETF: Mobile Ad-hoc Networks (MANET) Working Group, 2008. http://www.ietf.org/html.charters/manet-charter.html. pages 34, 51

[mr-cooperation-analysis] Tsukada Manabu, Kuntz Romain, and Ernst Thierry. *Analysis of Multiple Mobile Routers Cooperation*, October 2005. IETF work in progress, draft-tsukada-nemo-mr-cooperation-analysis-00. pages 44

[multipath-manet] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal. Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges, 2004. Performance Tools and Applications to Networked Systems, Lecture Notes in Computer Science Vol. 2965, Springer 2004, pp. 209-234. pages 35

[rfc2080] G. Malkin and R. Minnear. RIPng for IPv6. RFC 2080 (Proposed Standard), January 1997. pages 40

[rfc2460] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460 (Draft Standard), December 1998. Updated by RFCs 5095, 5722, 5871. pages 3

[rfc2578] K. McCloghrie, D. Perkins, and J. Schoenwaelder. Structure of Management Information Version 2 (SMIv2). RFC 2578 (Standard), April 1999. pages 90, 94, 95, 96

[rfc3077] E. Duros, W. Dabbous, H. Izumiyama, N. Fujii, and Y. Zhang. A Link-Layer Tunneling Mechanism for Unidirectional Links. RFC 3077 (Proposed Standard), March 2001. pages 33

[rfc3315] R. Droms, J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney. Dynamic Host Configuration Protocol for IPv6 (DHCPv6). RFC 3315 (Proposed Standard), July 2003. Updated by RFCs 4361, 5494. pages 38

[rfc3411] D. Harrington, R. Presuhn, and B. Wijnen. An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks. RFC 3411 (Standard), December 2002. Updated by RFCs 5343, 5590. pages 90

[rfc3561] C. Perkins, E. Belding-Royer, and S. Das. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561 (Experimental), July 2003. pages 35

[rfc3626] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626 (Experimental), October 2003. pages 34, 35, 40

[rfc3633] O. Troan and R. Droms. IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6. RFC 3633 (Proposed Standard), December 2003. pages 51

[rfc3684] R. Ogier, F. Templin, and M. Lewis. Topology Dissemination Based on Reverse-Path Forwarding (TBRPF). RFC 3684 (Experimental), February 2004. pages 35

[rfc3963] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. Network Mobility (NEMO) Basic Support Protocol. RFC 3963 (Proposed Standard), January 2005. pages 3, 24, 25, 41, 43

[rfc3972] T. Aura. Cryptographically Generated Addresses (CGA). RFC 3972 (Proposed Standard), March 2005. Updated by RFCs 4581, 4982. pages 41

[rfc4022] R. Raghunarayan. Management Information Base for the Transmission Control Protocol (TCP). RFC 4022 (Proposed Standard), March 2005. pages 90, 94

[rfc4087] D. Thaler. IP Tunnel MIB. RFC 4087 (Proposed Standard), June 2005. pages 90, 94

[rfc4113] B. Fenner and J. Flick. Management Information Base for the User Datagram Protocol (UDP). RFC 4113 (Proposed Standard), June 2005. pages 90, 94

[rfc4293] S. Routhier. Management Information Base for the Internet Protocol (IP). RFC 4293 (Proposed Standard), April 2006. pages 90, 92, 94

[rfc4295] G. Keeni, K. Koide, K. Nagami, and S. Gundavelli. Mobile IPv6 Management Information Base. RFC 4295 (Proposed Standard), April 2006. pages 91, 94

[rfc4651] C. Vogt and J. Arkko. A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization. RFC 4651 (Informational), February 2007. pages 41

[rfc4728] D. Johnson, Y. Hu, and D. Maltz. The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4. RFC 4728 (Experimental), February 2007. pages 35

[rfc4861] T. Narten, E. Nordmark, W. Simpson, and H. Soliman. Neighbor Discovery for IP version 6 (IPv6). RFC 4861 (Draft Standard), September 2007. pages 38, 51

[rfc4862] S. Thomson, T. Narten, and T. Jinmei. IPv6 Stateless Address Autoconfiguration. RFC 4862 (Draft Standard), September 2007. pages 38, 119

[rfc4866] J. Arkko, C. Vogt, and W. Haddad. Enhanced Route Optimization for Mobile IPv6. RFC 4866 (Proposed Standard), May 2007. pages 41

[rfc4885] T. Ernst and H-Y. Lach. Network Mobility Support Terminology. RFC 4885 (Informational), July 2007. pages 41

[rfc4886] T. Ernst. Network Mobility Support Goals and Requirements. RFC 4886 (Informational), July 2007. pages 41

[rfc4888] C. Ng, P. Thubert, M. Watari, and F. Zhao. Network Mobility Route Optimization Problem Statement. RFC 4888 (Informational), July 2007. pages 34, 48

[rfc4889] C. Ng, F. Zhao, M. Watari, and P. Thubert. Network Mobility Route Optimization Solution Space Analysis. RFC 4889 (Informational), July 2007. pages 34, 48

[rfc4960] R. Stewart. Stream Control Transmission Protocol. RFC 4960 (Proposed Standard), September 2007. pages 48

[rfc4980] C. Ng, T. Ernst, E. Paik, and M. Bagnulo. Analysis of Multihoming in Network Mobility Support. RFC 4980 (Informational), October 2007. pages 34, 44

[rfc5184] F. Teraoka, K. Gogo, K. Mitsuya, R. Shibui, and K. Mitani. Unified Layer 2 (L2) Abstractions for Layer 3 (L3)-Driven Fast Handover. RFC 5184 (Experimental), May 2008. pages 47

[rfc5201] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson. Host Identity Protocol. RFC 5201 (Experimental), April 2008. pages 43, 48

[rfc5213] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil. Proxy Mobile IPv6. RFC 5213 (Proposed Standard), August 2008. pages 43

[rfc5340] R. Coltun, D. Ferguson, J. Moy, and A. Lindem. OSPF for IPv6. RFC 5340 (Proposed Standard), July 2008. pages 40

[rfc5380] H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier. Hierarchical Mobile IPv6 (HMIPv6) Mobility Management. RFC 5380 (Proposed Standard), October 2008. pages 43, 47, 50, 112

[rfc5488] S. Gundavelli, G. Keeni, K. Koide, and K. Nagami. Network Mobility (NEMO) Management Information Base. RFC 5488 (Proposed Standard), April 2009. pages 91, 94

[rfc5522] W. Eddy, W. Ivancic, and T. Davis. Network Mobility Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks. RFC 5522 (Informational), October 2009. pages 48

[rfc5533] E. Nordmark and M. Bagnulo. Shim6: Level 3 Multihoming Shim Protocol for IPv6. RFC 5533 (Proposed Standard), June 2009. pages 44, 48

[rfc5555] H. Soliman. Mobile IPv6 Support for Dual Stack Hosts and Routers. RFC 5555 (Proposed Standard), June 2009. pages 43

[rfc5568] R. Koodli. Mobile IPv6 Fast Handovers. RFC 5568 (Proposed Standard), July 2009. pages 43, 47

[rfc5648] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami. Multiple Care-of Addresses Registration. RFC 5648 (Proposed Standard), October 2009. pages 41, 44

[rfc5944] C. Perkins. IP Mobility Support for IPv4, Revised. RFC 5944 (Proposed Standard), November 2010. pages 17

[rfc6088] G. Tsirtsis, G. Giarreta, H. Soliman, and N. Montavont. Traffic Selectors for Flow Bindings. RFC 6088 (Proposed Standard), January 2011. pages 47, 103

[rfc6089] G. Tsirtsis, H. Soliman, N. Montavont, G. Giaretta, and K. Kuladinithi. Flow Bindings in Mobile IPv6 and Network Mobility (NEMO) Basic Support. RFC 6089 (Proposed Standard), January 2011. pages 47, 103

[rfc6106] J. Jeong, S. Park, L. Beloeil, and S. Madanapalli. IPv6 Router Advertisement Options for DNS Configuration. RFC 6106 (Proposed Standard), November 2010. pages 112

[rfc6275] C. Perkins, D. Johnson, and J. Arkko. Mobility Support in IPv6. RFC 6275 (Proposed Standard), July 2011. pages 17, 24, 25, 40, 41, 43, 48, 195

[rfc6281] S. Cheshire, Z. Zhu, R. Wakikawa, and L. Zhang. Understanding Apple's Back to My Mac (BTMM) Service. RFC 6281 (Informational), June 2011. pages 43

[rfc6301] Z. Zhu, R. Wakikawa, and L. Zhang. A Survey of Mobility Support in the Internet. RFC 6301 (Informational), July 2011. pages 34, 42

List of Figures

List of Tables

List of Acronyms

2G 2nd Generation mobile telecommunications

3G 3rd Generation mobile telecommunications

AP Access Point

AR Access Router

ASN.1 Abstract Syntax Notation One

AU Application Unit

BA Binding Acknowledgement

BC Binding Cache

BE Binding Error

BID Binding Identification number

BU Binding Update

BUL Binding Update List

C2C-CC Car-to-Car Communication Consortium

C2CNet Car-to-Car Network

CALM Communications Architecture for Land Mobile

CAM Co-operative Awareness Messages

CCU Communication and Control Unit

CDMA Code Division Multiple Access

CE Correspondent Entity

CEN European Committee for Standardization

CI Communication Interface

CIMAE Communication Interface Management Adaptation Entity

CN Correspondent Node

CoA Care-of Address

CoT Care-of Test

CoTI Care-of Test Init

DAD Duplicated Address Detection

DENM Decentralized environmental Notification Messages

DHAAD Dynamic Home Agent Address Discovery

DHCP Dynamic Host Configuration Protocol

DNS Domain Name System

DSRC Dedicated Short Range Communications

EC European Commission

ETSI European Telecommunications Standards Institute

FM Frequency Modulation

FMIPv6 Fast Handovers for Mobile IPv6

FP6 Sixth Framework Programme

FP7 Seventh Framework Programme

GPRS General Packet Radio Service

GPS Global Positioning System

GPSR Greedy Perimeter Stateless Routing

GSM Global System for Mobile communications

HA Home Agent

HIP Host Identity Protocol

HMIPv6 Hierarchical Mobile IPv6

HNA Host and Network Association

HoA Home Address

HoT Home Test

HoTI Home Test Init

HSPA High Speed Packet Access

I2V Infrastructure-to-Vehicle

ICMPv6 Internet Control Message Protocol version 6

ICT Information Communication Technologies

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

IME Interface Management Entity

IPFR IP Filter Rule

ISO International Organization for Standardization

ITS-S ITS Station

ITS Intelligent Transportation Systems

ITU International Telecommunication Union

L2 Layer 2

L2TP Layer-2 Tunneling Protocol

L3 Layer 3

LAN Local Area Network

LDM Local Dynamic Map

LLC Logical Link Control

LTE Long Term Evolution

LS Location Service

LT Location Table

MAC Medium Access Control

MADM Multiple Attribute Decision Making

MAN Metropolitan Area Network

MANET Mobile Ad-hoc Network

MAP Mobility Anchor Point

MCoA Multiple Care-of Addresses Registration

MIB Management Information Base

MLME MAC Layer Management Entity

MN Mobile Node

MNN Mobile Network Node

MNP Mobile Network Prefix

MNPP Mobile Network Prefix Provisioning

MR Mobile Router

MTU Maximum Transmission Unit

NA Neighbor Advertisement

NDP Neighbor Discovery Protocol

NEMO Network Mobility

NEPL NEMO Platform for Linux

NMEA National Marine Electronics Association

NS Neighbor Solicitation

NTP Network Time Protocol

OBU On-Board Unit

OLSR Optimized Link State Routing

OSI Open Systems Interconnection

OSPF Open Shortest Path First

PAN Personal Area Network

PDR Packet Delivery Ratio

PFBU Peer Flow Binding Update

PHY Physical

PLME PHY Layer Management Entity

PMIP Proxy Mobile IPv6

PPP Point-to-Point Protocol

QoS Quality of Service

RA Router Advertisement

RADVD Router Advertisement Daemon

RDS Radio Data System

RIPng Routing Information Protocol

RO Route Optimization

RPDB Routing Policy Database

RS Router Solicitation

RSSI Received Signal Strength Indication

RSU Road Side Unit

RTT Round-Trip Time

SAM Service Advertisement Message

SAP Service Access Point

SAW Simple Additive Weighing

SCTP Stream Control Transmission Protocol

SHIM6 Level 3 Multihoming Shim Protocol for IPv6

SHIM6 Site Multihoming by IPv6 Intermediation

SLAAC Stateless address autoconfiguration

SME ITS Station Management Entity

SMIv2 Structure of Management Information Version 2

SNMP Simple Network Management Protocol

SNT ITS Station Network and Transport layer

SPI Security Parameter Index

TC204 WG16 Technical Committee 204 Working Group 16

TCP Transmission Control Protocol

UDP User Datagram Protocol

UMTS Universal Mobile Telecommunications System

UTC Coordinated Universal Time

V2C Vehicle-to-Center

V2I Vehicle-to-Infrastructure

V2R Vehicle-to-Roadside

V2V Vehicle-to-Vehicle

VANET Vehicular Ad-hoc Network

VCI Virtual Communication Interface

WAVE Wireless Access in Vehicular Environments

WG Working Group

WGS-84 World Geodetic System 84

WIMAX Worldwide Interoperability for Microwave Access

WLAN Wireless Local Area Network

WSMP WAVE Short Message Protocol

XML Extensible Markup Language

Index

Gestion des communications dans les systèmes de transport intelligents coopératifs

Résumé :

Les systèmes de transport intelligents (STI) coopératifs) sont des systèmes où les véhicules, l'infrastructure routière, les centres de contrôle de trafic et d'autres entités échangent des informations afin d'assurer une meilleure sécurité routière, l'efficacité du trafic et le confort des usagers de la route. Cet échange d'information doit s'appuyer sur une référence d'architecture de communication commune. C'est dans ce but que l'architecture de station STI a été spécifié par l'ISO et l'ETSI. Le concept de cette architecture de référence permet aux stations STI-véhicules et stations STI-infrastructure de s'organiser dans un réseau véhiculaire ad-hoc (VANET), tout en utilisant des protocoles de communication tels qu'GeoNetworking IPv6 et IEEE802.11p ainsi que toute autre technologie d'accès afin de se connecter de manière transparente à Internet. Plusieurs chemins peuvent donc être accessible à une station STI véhicule pour communiquer avec d'autres stations STI. Les chemins sont de trois types : le chemin direct, le chemin optimisé et le chemin d'ancré.

L'objectif de cette étude est d'optimiser la communication entre stations STI en sélectionnant le meilleur chemin de communication disponible.. Cela exige d'abord de recueillir les informations disponibles localement dans la station STI (la position, la vitesse, les exigences des applications, les caractéristiques des supports de communication, les capacités, l'état du chemin), ainsi que les informations des stations STI voisines (position, vitesse, services, etc.). Ces informations sont ensuite traitées par le biais d'un algorithme de prise de décision. Premièrement, nous définissons un module réseau qui permet la combinaison d'IPv6 avec le GeoNetworking. Deuxièmement, nous proposons un module de gestion inter-couche pour la sélection du meilleur chemin. Nos contributions s'intègrent dans l'architecture de station STI par la définition de la relation entre la couche réseau et transport (qui héberge la contribution GeoNetworking IPv6) et l'entité verticale de gestion inter-couche (qui accueille l'algorithme de décision pour la sélection de chemin). Nous avons spécifiés les fonctions permettant l'échange de paramètres par l'intermédiaire de la SAP (Service Access Point) entre la couche réseau et l'entité de gestion (MN-SAP). Les paramètres utilisés dans l'entité de gestion inter-couche sont extraits d'une manière agnostique par rapport aux protocoles de la couche réseau et transport, ce qui permet de remplacer facilement les éléments d'une couche sans affecter les autres (par exemple, remplacer NEMO par une autre protocole de mobilité) et de permuter plusieurs piles réseau (on peut choisir d'utiliser la pile IPv6 ou bien la pile GeoNetworking, ou encore une combinaison des deux à la fois ou même une autre pile).

Mots clés : l'architecture de station STI, IPv6, GeoNetworking, sélection de chemin, multi-connexion

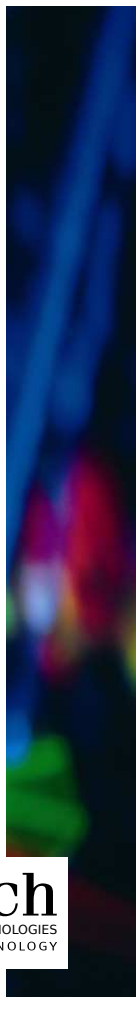
Communications Management in Cooperative Intelligent Transportation Systems

Abstract:

Cooperative Intelligent Transportation Systems (Cooperative ITS) are systems where the vehicles, the roadside infrastructure, central control centers and other entities exchange information in order to achieve better road safety, traffic efficiency and comfort of the road users. This exchange of information must rely on a common communication architecture. The ITS Station reference architecture has thus been specified in ISO and ETSI. It allows vehicles and roadside ITS stations to organize themselves into Vehicular Ad-hoc Network (VANET), presumably though IPv6 GeoNetworking using IEEE802.11p and to connect seamlessly to the Internet though any available access technology. Several paths may thus be available at a given vehicle ITS station to communicate with other ITS stations. Paths are of three types: direct path, optimize path and anchor path.

The objective of the study is to optimize the communication between ITS Stations by selecting the best available communication path. This requires first to gather information available locally at the ITS station (position, speed, application requirements, media characteristics, capabilities, path status, ...) and collected from neighbors ITS stations (position, speed, services, ...) and then to process this information through a decision-making algorithm. First, we define a network module allowing the combination of IPv6 together with GeoNetworking. Second, we propose a cross-layer path selection management module. Our contributions are mapped to the ITS station reference architecture by defining the relation between the ITS station network and transport layer (which hosts our IPv6 GeoNetworking contribution) and the vertical ITS station cross-layer entity (which hosts the path decision-making algorithm). We specify the functions allowing the exchange of parameters through the Service Access Point (SAP) between the network layer and the management entity (MN-SAP). The parameters used at the cross layer ITS station management entity are abstracted in a way so that they are agnostic to the protocols used at the ITS station network and transport layer, therefrom allowing easy replacement of protocol elements (e.g. replacing NEMO by other mobility support protocol) or permutation of the network stack (IPv6 or GeoNetworking, a combination of both or other network stack).

Keywords: ITS Station Architecture, IPv6, GeoNetworking, Path Selection, Multihoming



MINES ParisTech

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY